Wireless Security

Overview of Wireless, Securing Wireless, Evolution of WiFi and Perspectives on the Future

3rd Annual Security Symposium
Kansas City Security Coalition
24 June 2003 – Kansas City

Leslie D. Owens, Booz Allen Hamilton

"Those who cannot remember the past are condemned to repeat it."

George Santayana, 1863 - 1952
Spanish-born American poet and philosopher
The Life of Reason

Presenter Information

Leslie D. Owens (Les)

Booz Allen Hamilton, Wireless Security Lead

703/902-7091 (office)

703/980-3877 (cellular)

Owens_les@ bah.com (email)

les.owens@att.net

Presentation Outline

- Introduction to Wireless
- Wireless Security Fundamentals
- A Quick Look Back at First Generation Cellular
- 802.11 Technology and Security (features, vulnerabilities and solutions)
- Comprehensive Wireless Security Solutions
- Future Wireless
- Lessons Learned for Wireless
- Discussion

Introduction to Wireless

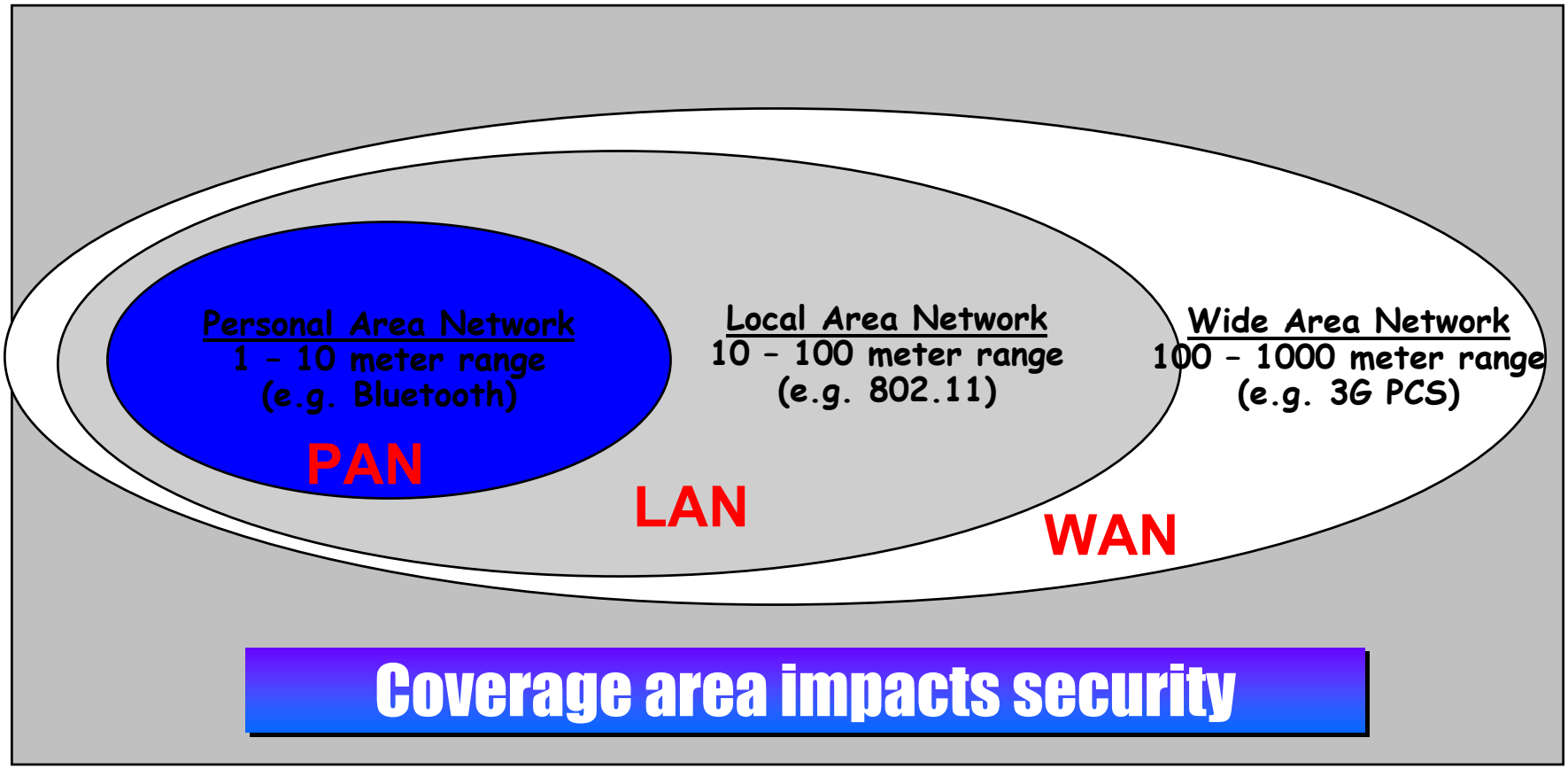
What is all this wireless stuff anyway?

Wireless Technology Alternatives

- Bluetooth
- 802.11a, b, g
- Wireless IP
- 2.5/3G Cellular
- Ad Hoc Networks
- WAP
- GPRS
- Hyperlan2 /HomeRF
- SMS
- Mobile IP
- Satellite
- UWB
- 802.16
- Blackberry
- CDPD
- MANETs
- Software Defined Radio
- 802.20

Wireless is more than cellular and 802.11

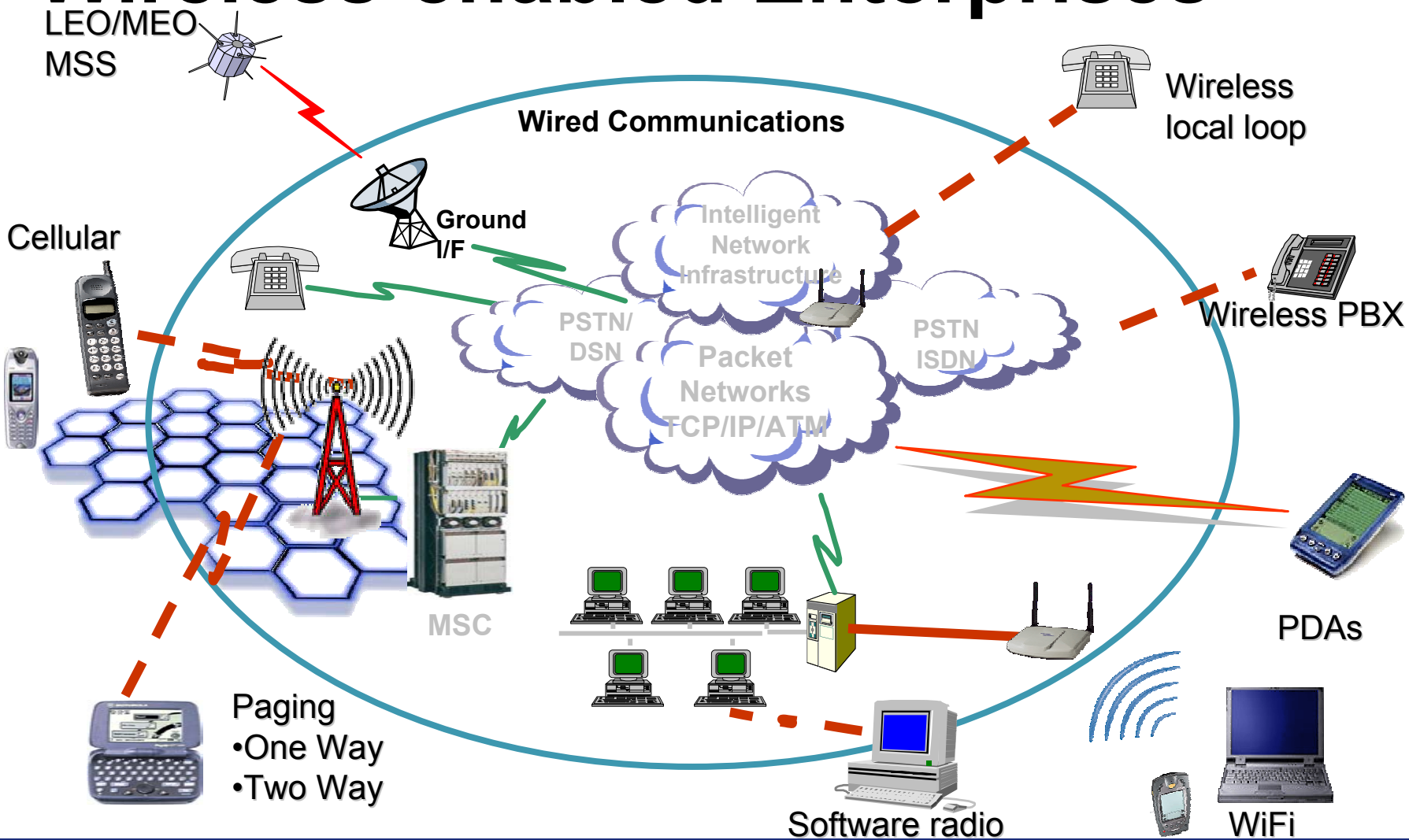
Coverage Area for PAN, LAN and WAN



What the deal with wireless?

- Involves transmitting data between devices that are not physically connected
- Devices range from PDAs to pagers to smart phones to sensors to satellites
- Coverage ranges from a few feet to large very large geographic areas
- Speeds range from low to very high

Wireless-enabled Enterprises



Wireless Security Fundamentals

What's Different About Wireless Security?

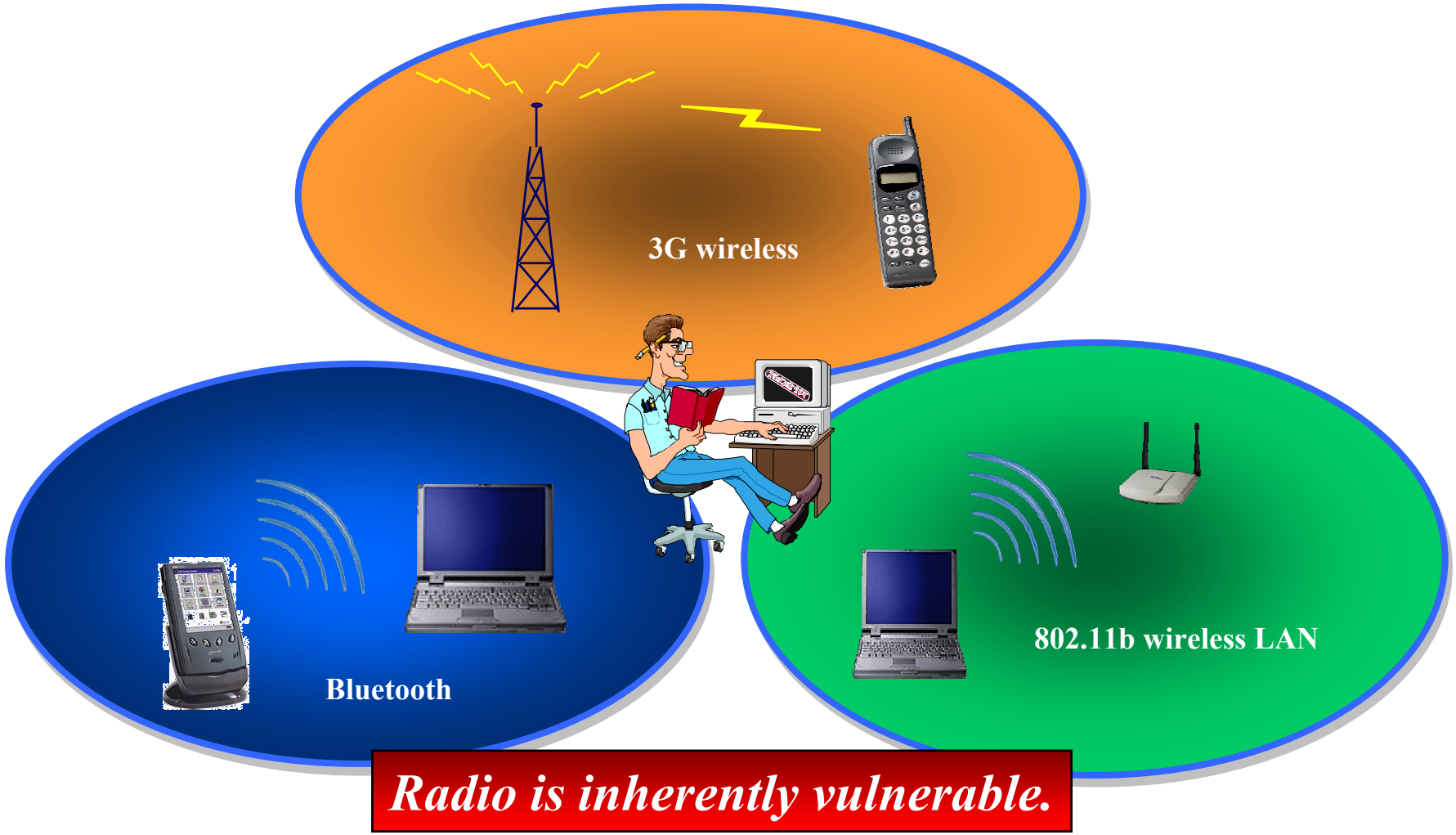
- **Physical security** – barriers, walls, fences – can often be used to limit access to a wired network
- **Radio frequencies** are not constrained by most physical barriers
  - Anyone within proximity may be able to gain access (without detection)
  - Additional countermeasures may be required

Wireless Security Fundamentals

Wireless security needed at three points:

- Wireless device
- During transmission
- At end-point (workstation, gateway, or other wireless device)

Wireless Means Radio



Radio is inherently vulnerable.

Wireless Threats and Vulnerabilities

If cryptography is absent or poorly implemented, adversaries may:

- Easily eavesdrop on wireless communications without detection
- Gain unauthorized access to a wired network
- Modify data in transit and violate integrity
- Capture and replay data that has already been sent

With wireless, jamming or DoS may be particularly easy

Practical Attacks

- Criminal steals a PDA with sensitive, confidential information
- A hacker gains access through 802.11 APs to launch other attacks
- Thief steals a wireless device to get free wireless service
- Vandal writes a virus and disseminates
- A foreign government with readily available 802.11 tools sniffs confidential information for industrial espionage

Issues with wireless

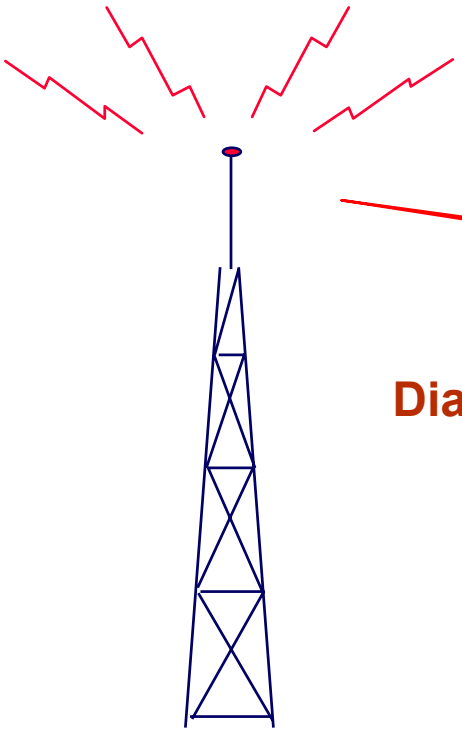
- They generally are **low power**
- They generally have **slower processors**
- They generally have **limited storage** capability

These effect the applications that can run and sometimes impacts the security of the device

A Quick Look Back at First Generation Cellular

First Generation Cellular ID System

Wireless Interface (Radio Path)

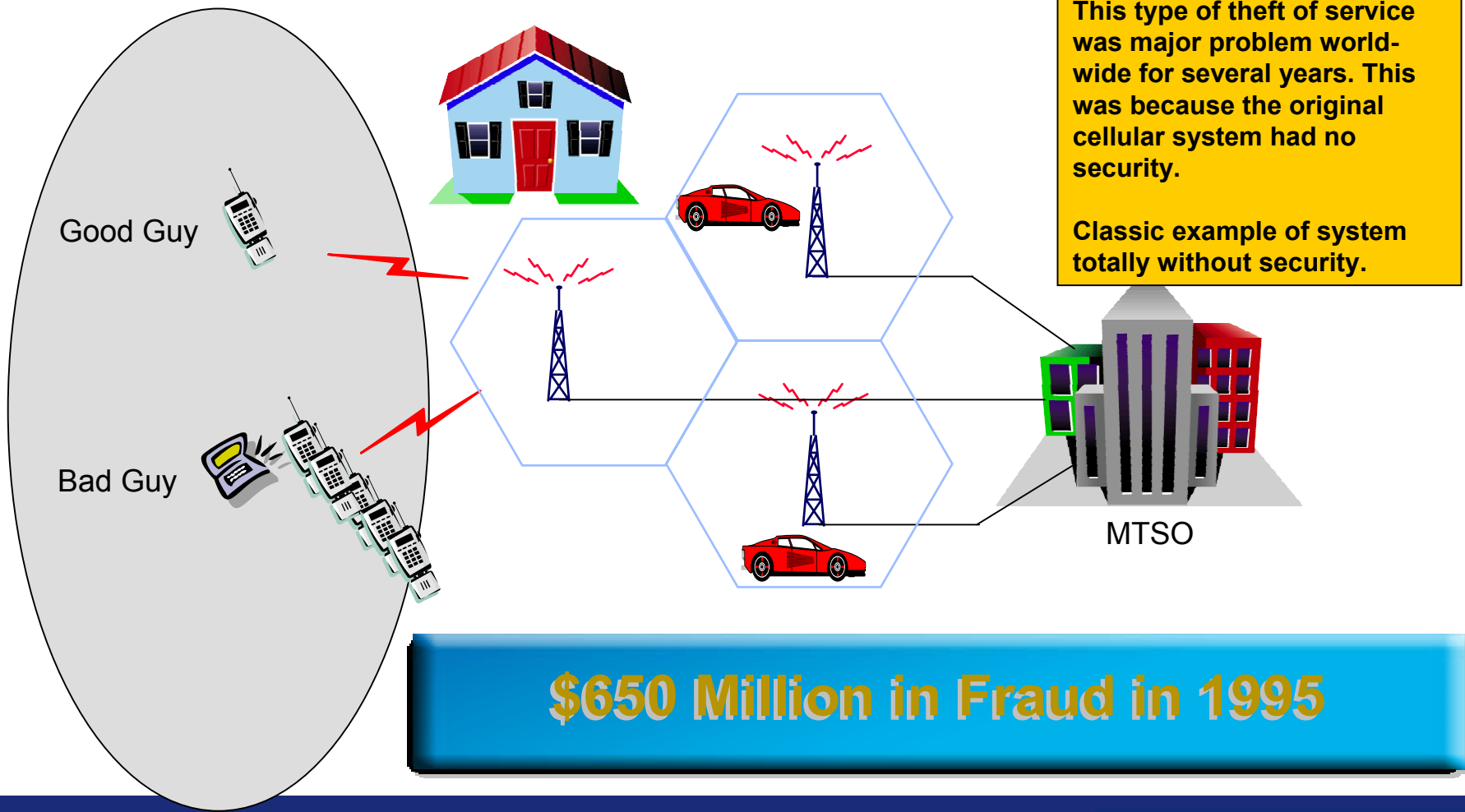


ESN: 82345AC5
MIN: 703-835-2902

Dialed digits: (212)-731-4321

Subscriber

Wireless Fraud Was a Major Problem



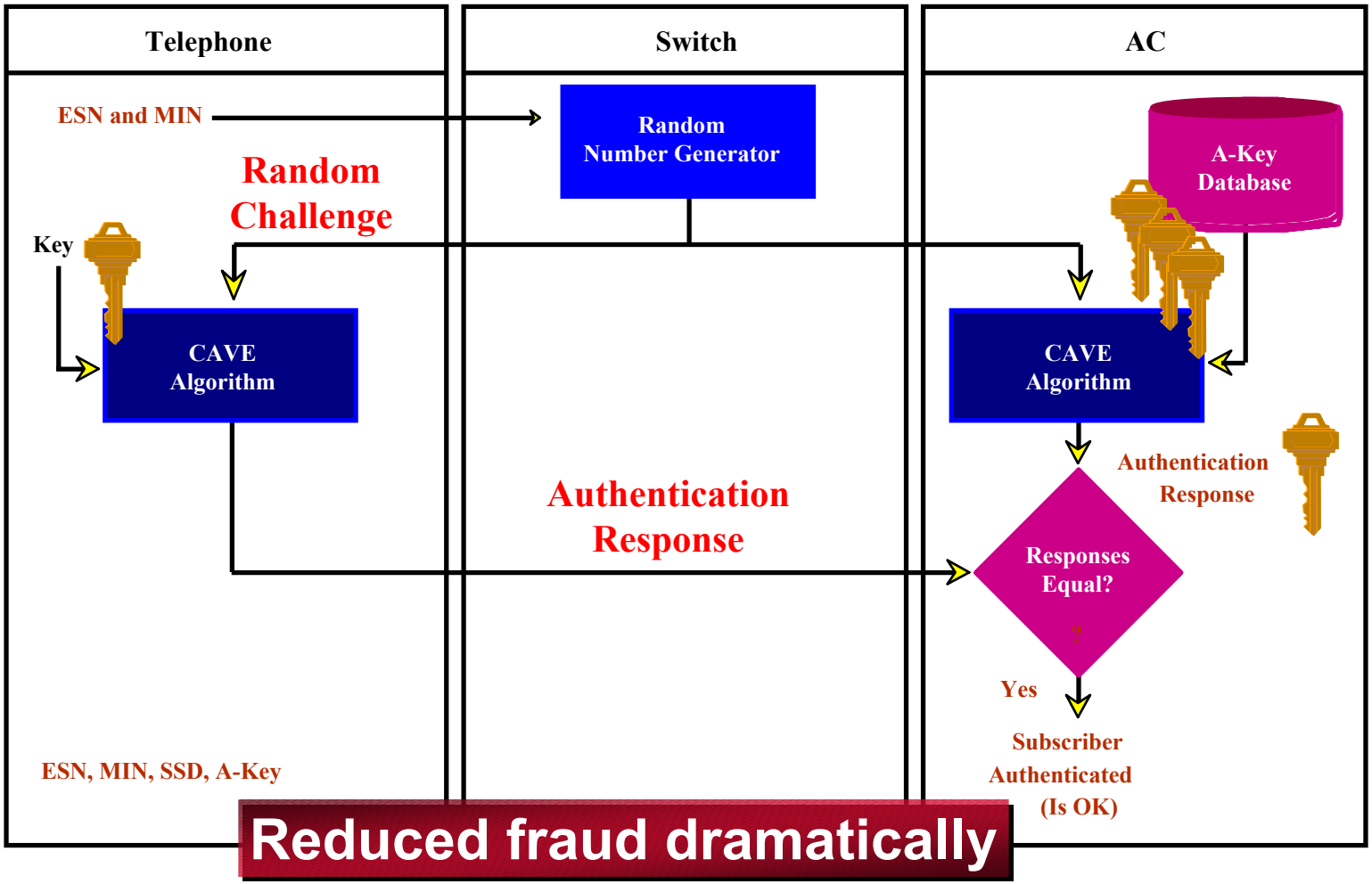
Clone Fraud

This type of theft of service was major problem world-wide for several years. This was because the original cellular system had no security.

Classic example of system totally without security.

$650 Million in Fraud in 1995

Principle of Cellular Authentication



802.11 Technology

WiFi and 802.11 will be used interchangeably

802.11 Architectural Components

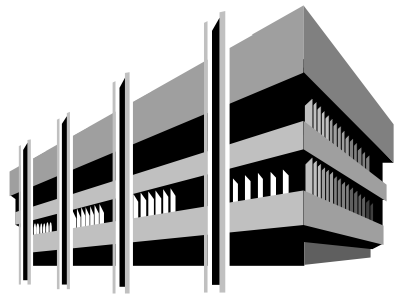
User Machine
(with client adapter)

Access Point

Ubiquity of WiFi

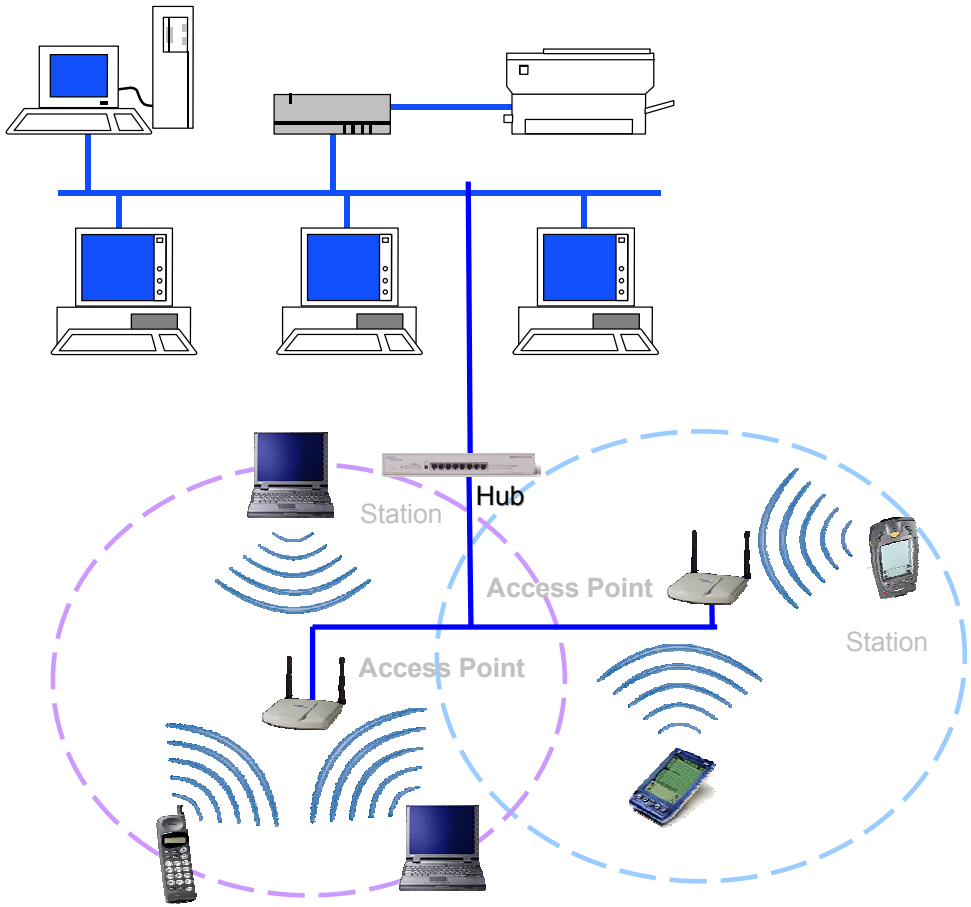
Residential

Corporations

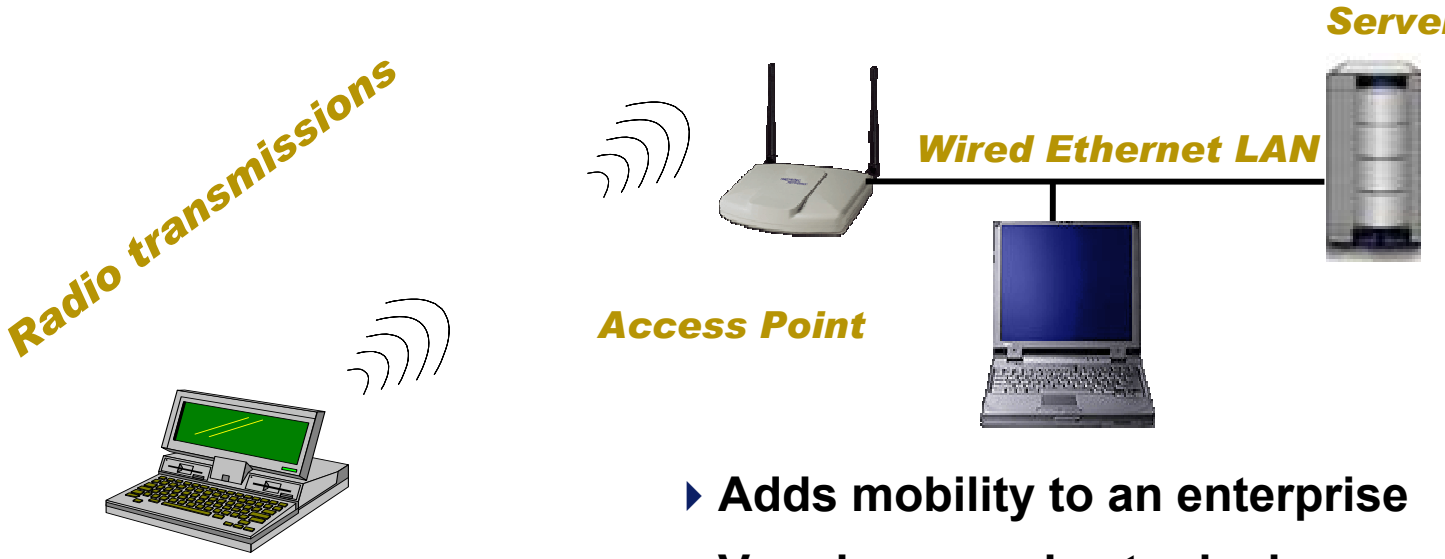


Universities and Hospitals

802.11 Technology Quickly Extends LAN



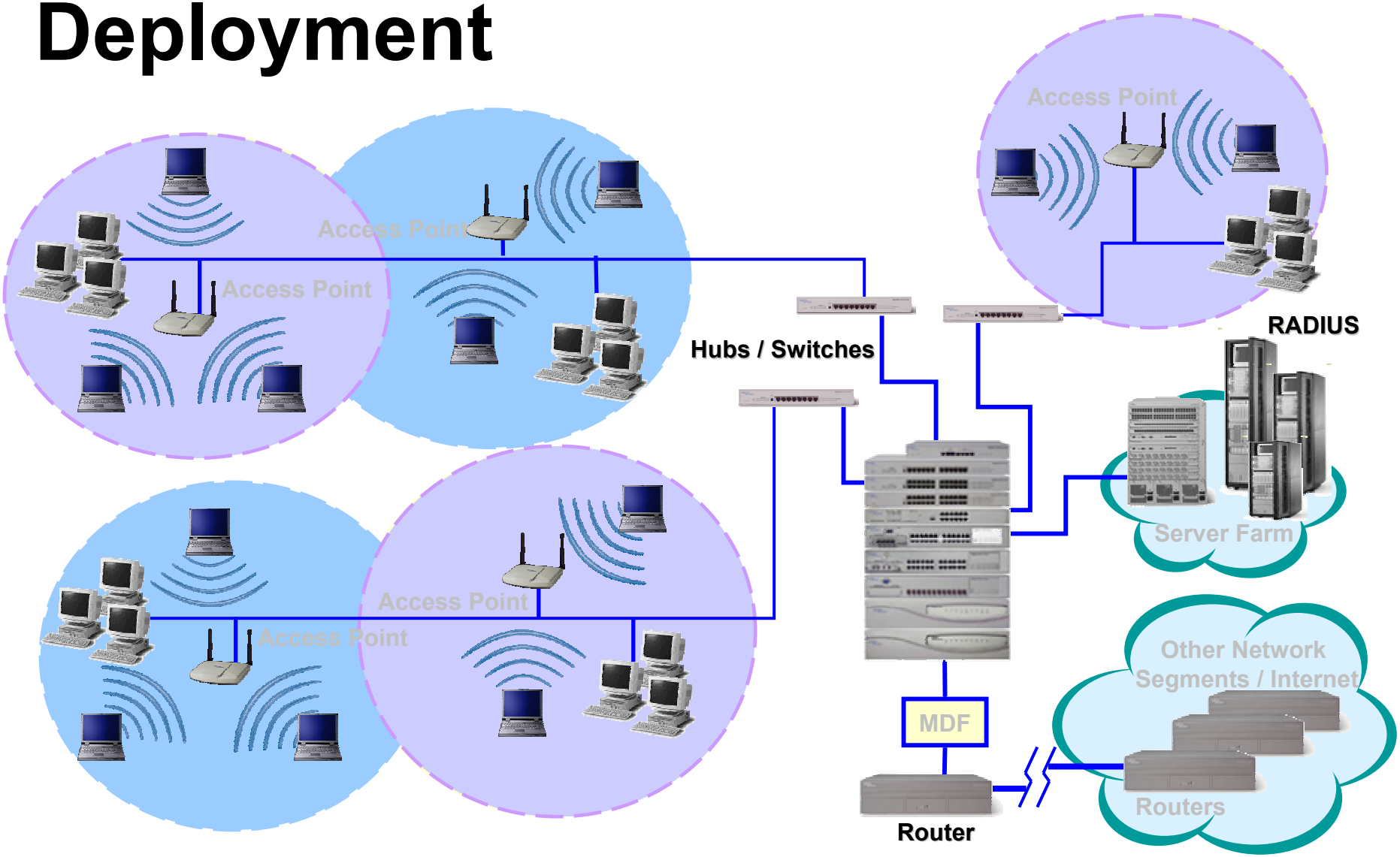
802.11 Wireless LAN Benefits



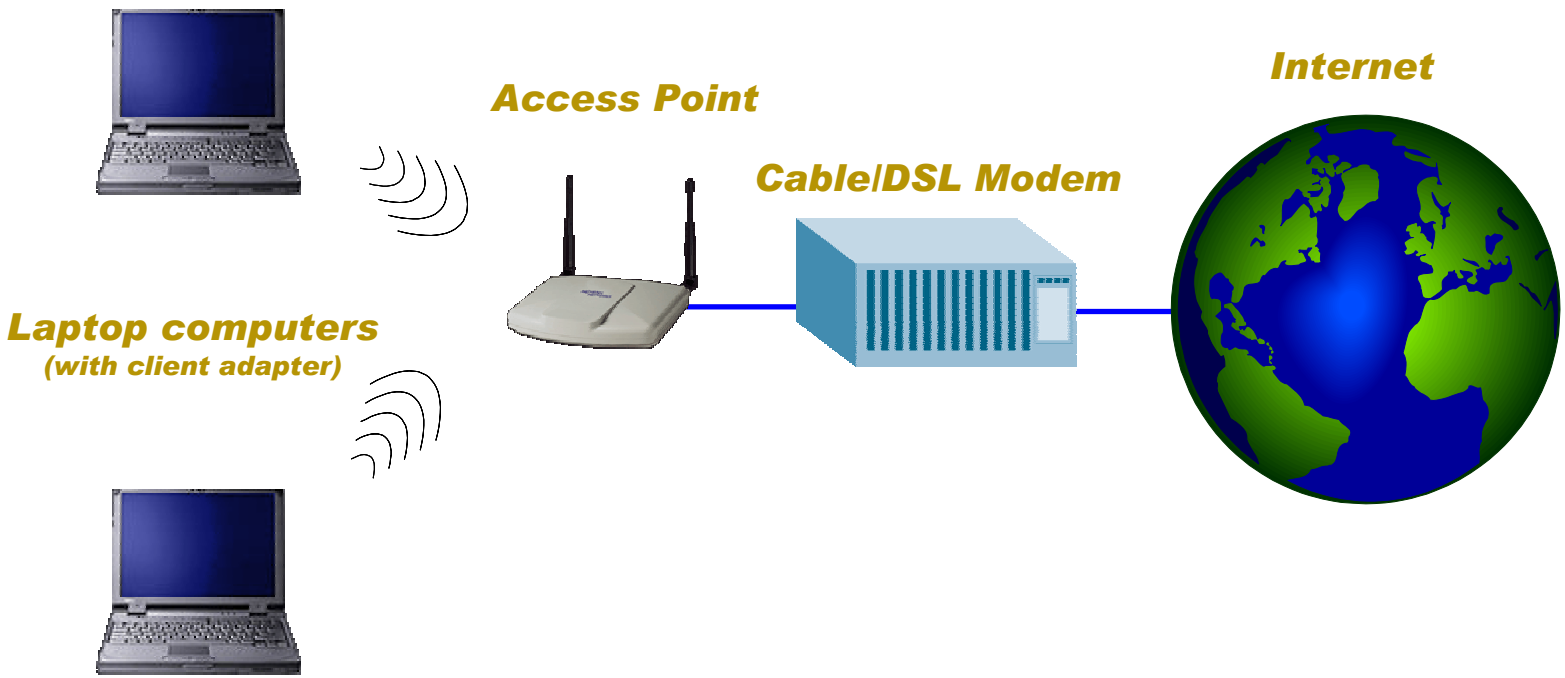
- Adds mobility to an enterprise
- Very inexpensive to deploy
- May be deployed very quickly
- May get very good performance – same as wired LAN
- Avoids wiring hassles in older buildings
- Facilitates changing organizations

802.11a/b are experiencing explosive growth

Typical Enterprise 802.11 Deployment

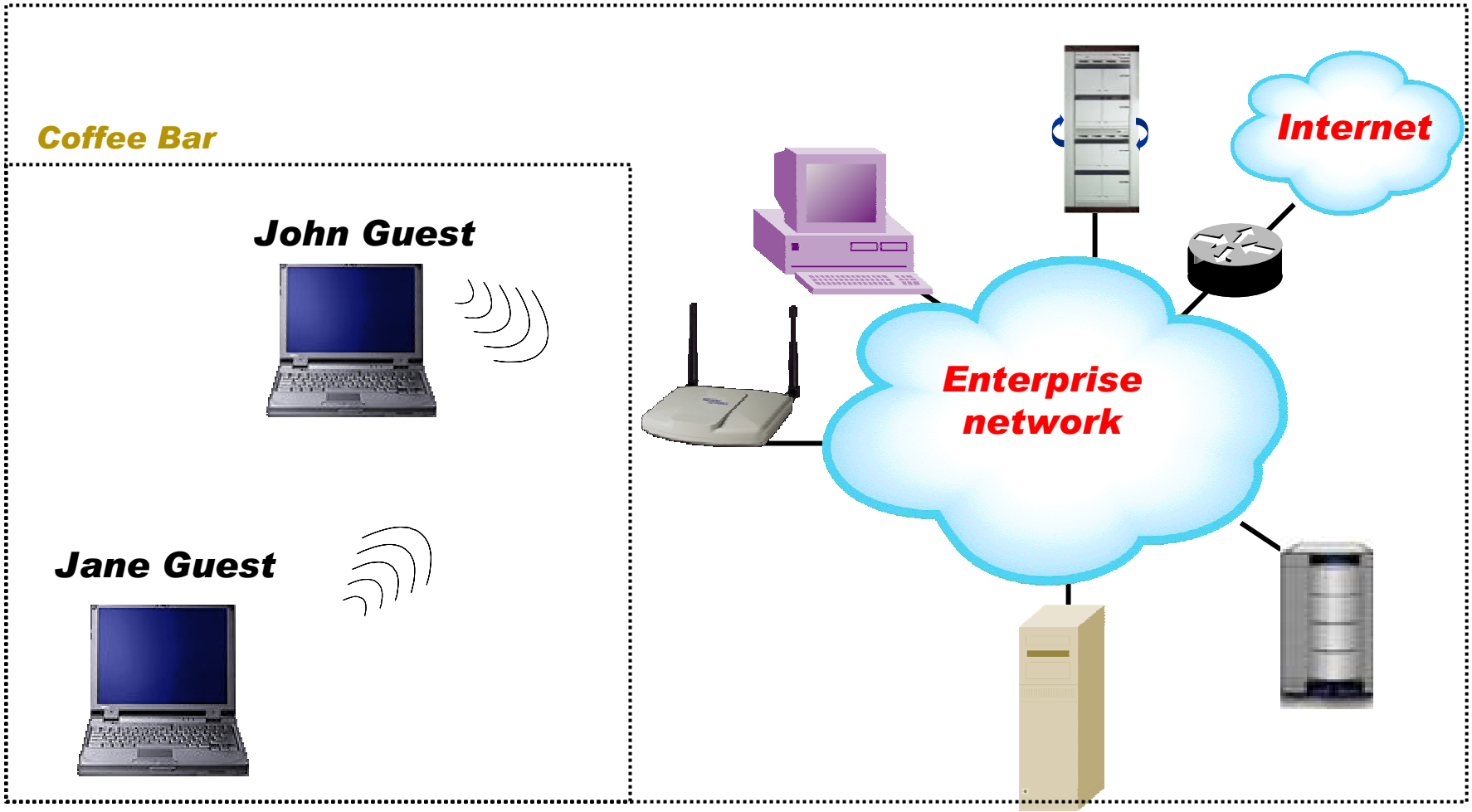


Typical Residential 802.11 Deployment



Hotspot – Coffee Shop

Joe's Best Coffee Corp.

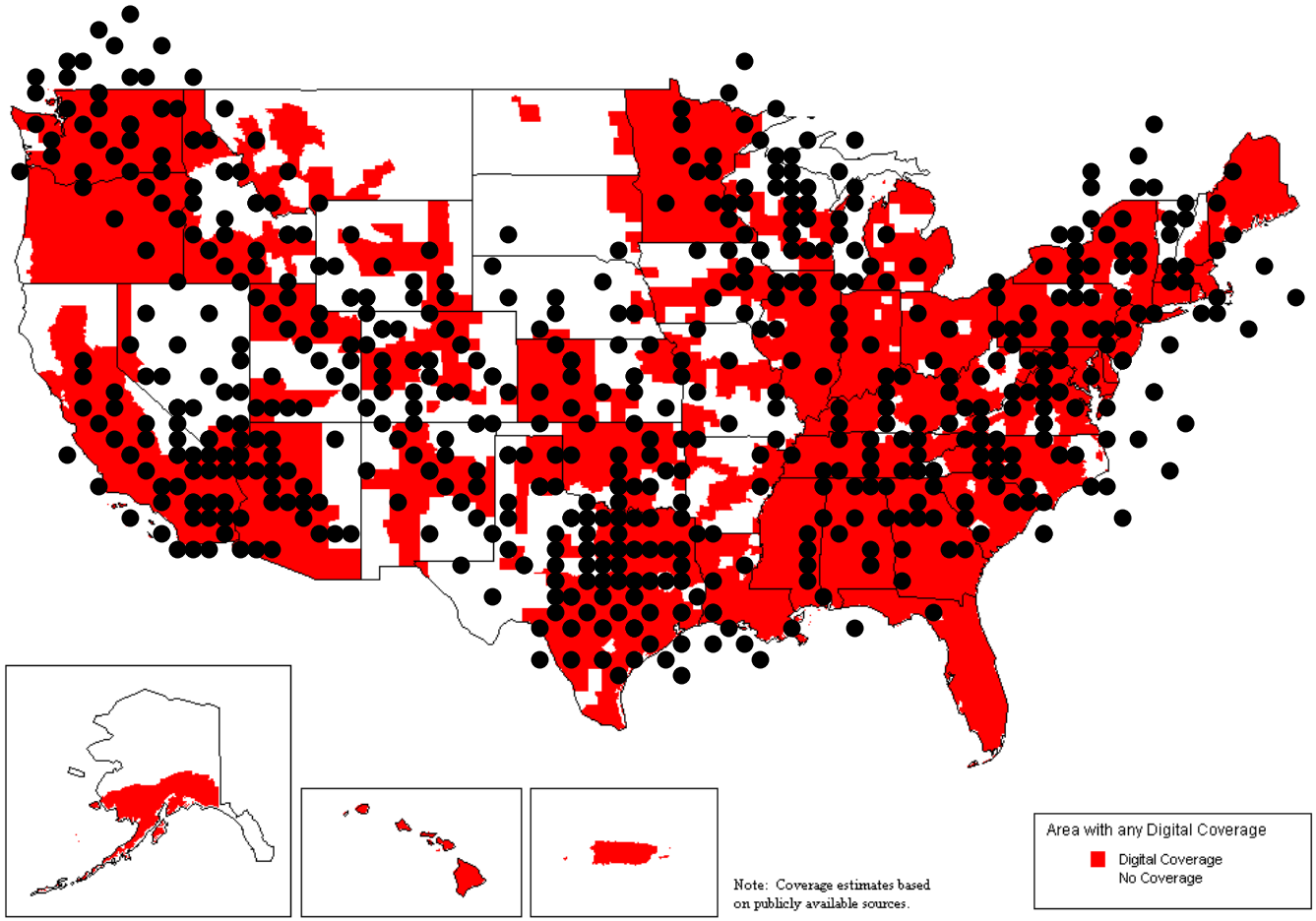


Some Statistics

- 67% of the world's largest companies will use WiFi networks by the end of 2004
- 90 million WiFi-enabled devices by 2007
- Today 3700 hotspots exist
- By 2004, 12,000 hotspots
- By 2007, 41,000 hotspots

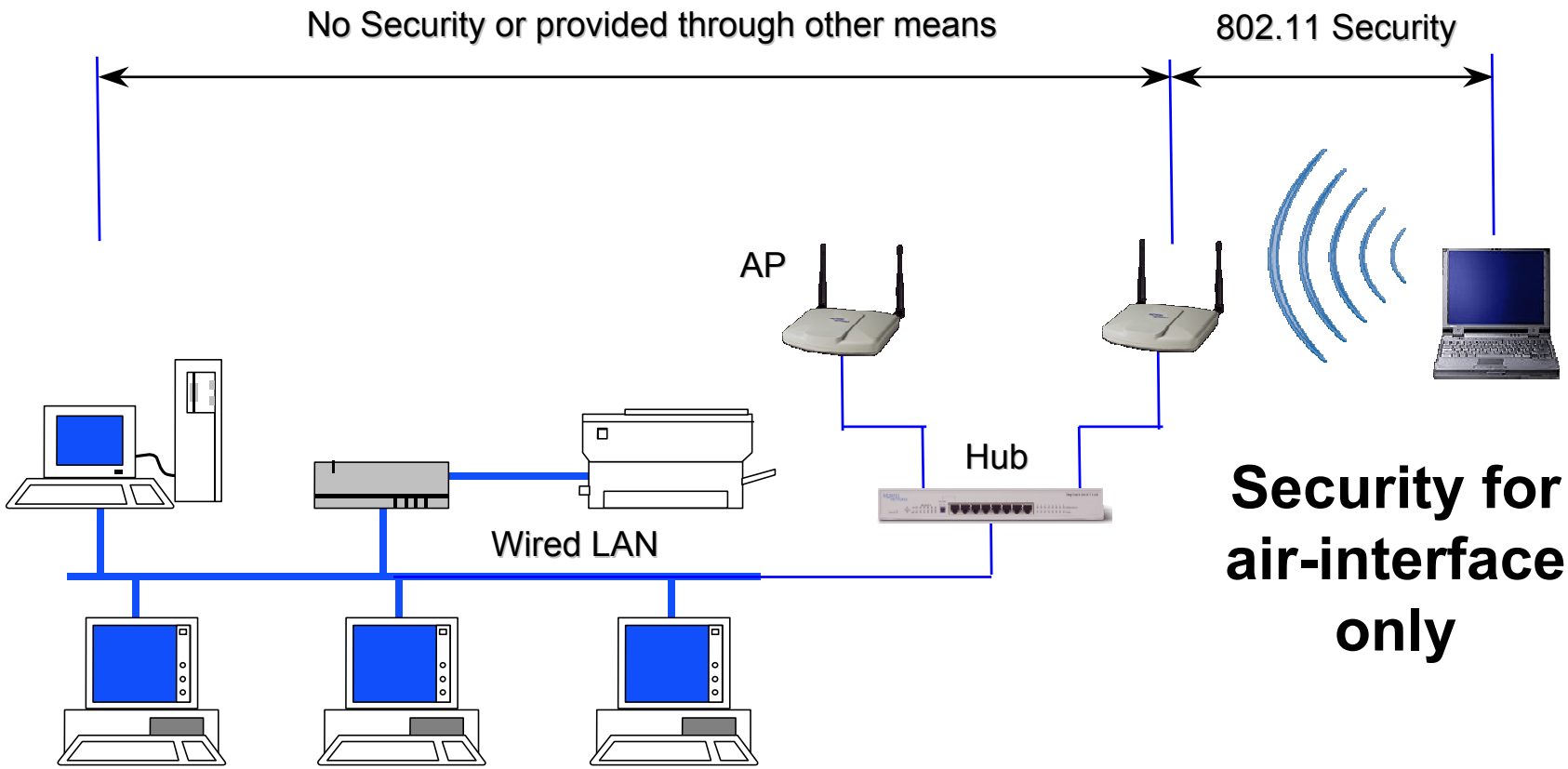
WiFi is definitely burgeoning

WiFi Hotspots – 2005



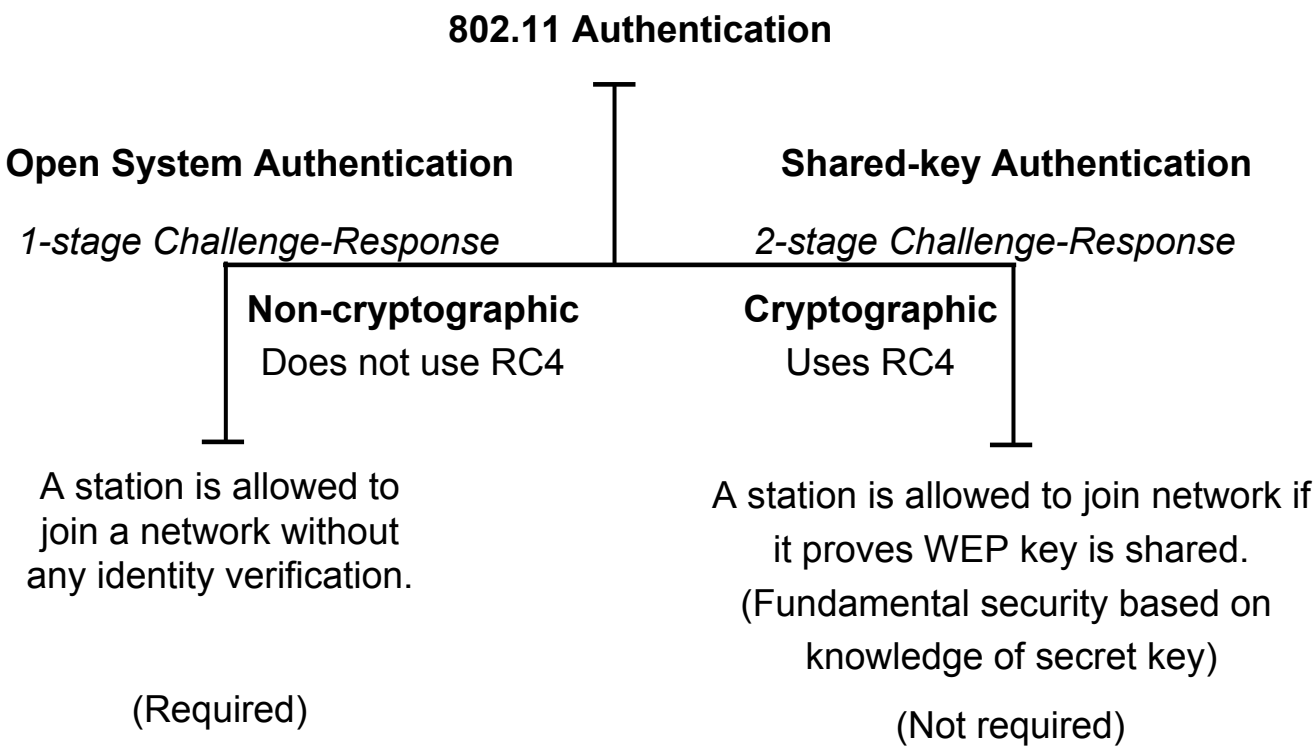
802.11 Security Features

802.11 WLAN Security

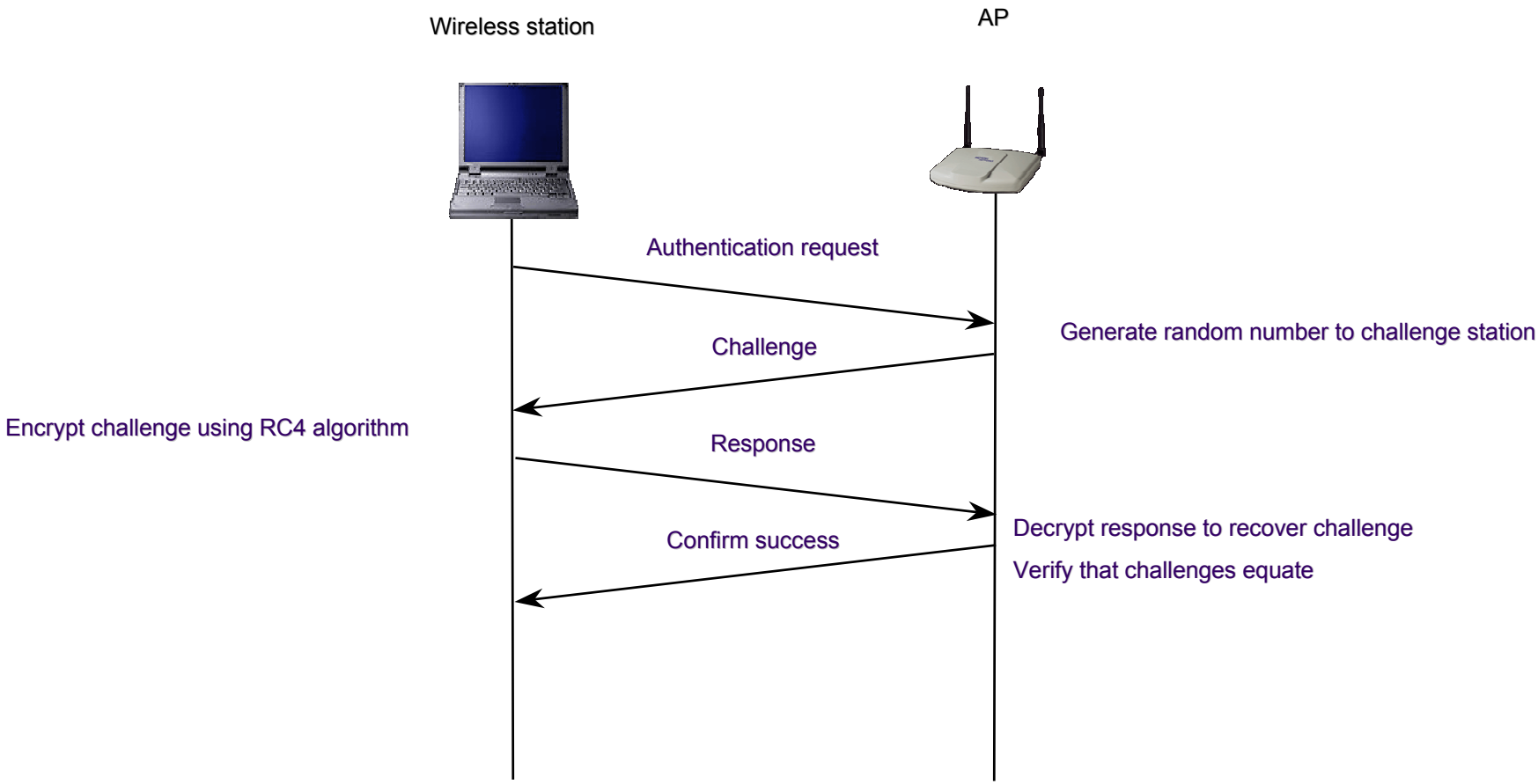


Security for air-interface only

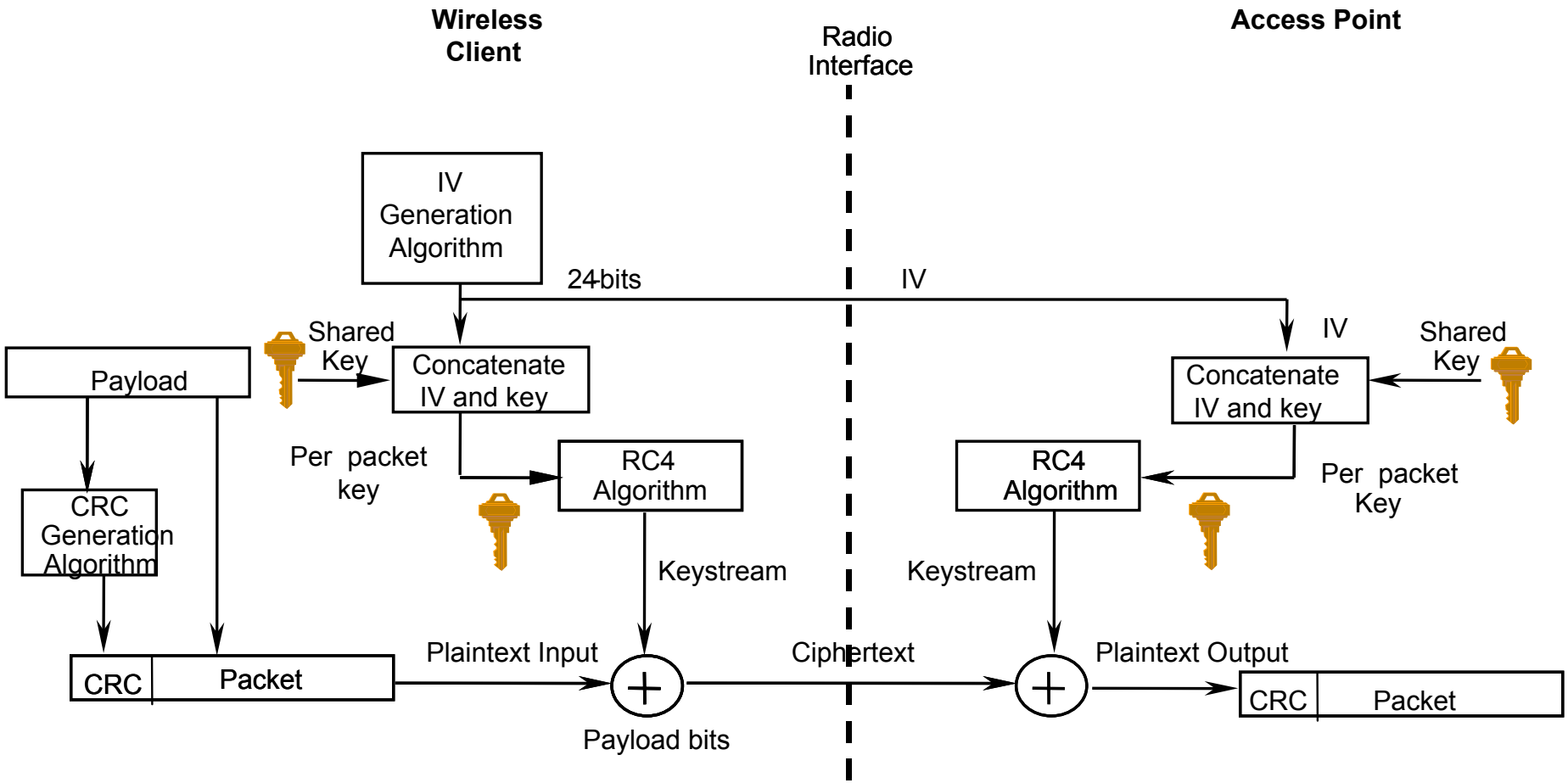
Types of WiFi Authentication



WiFi Shared-Key Authentication

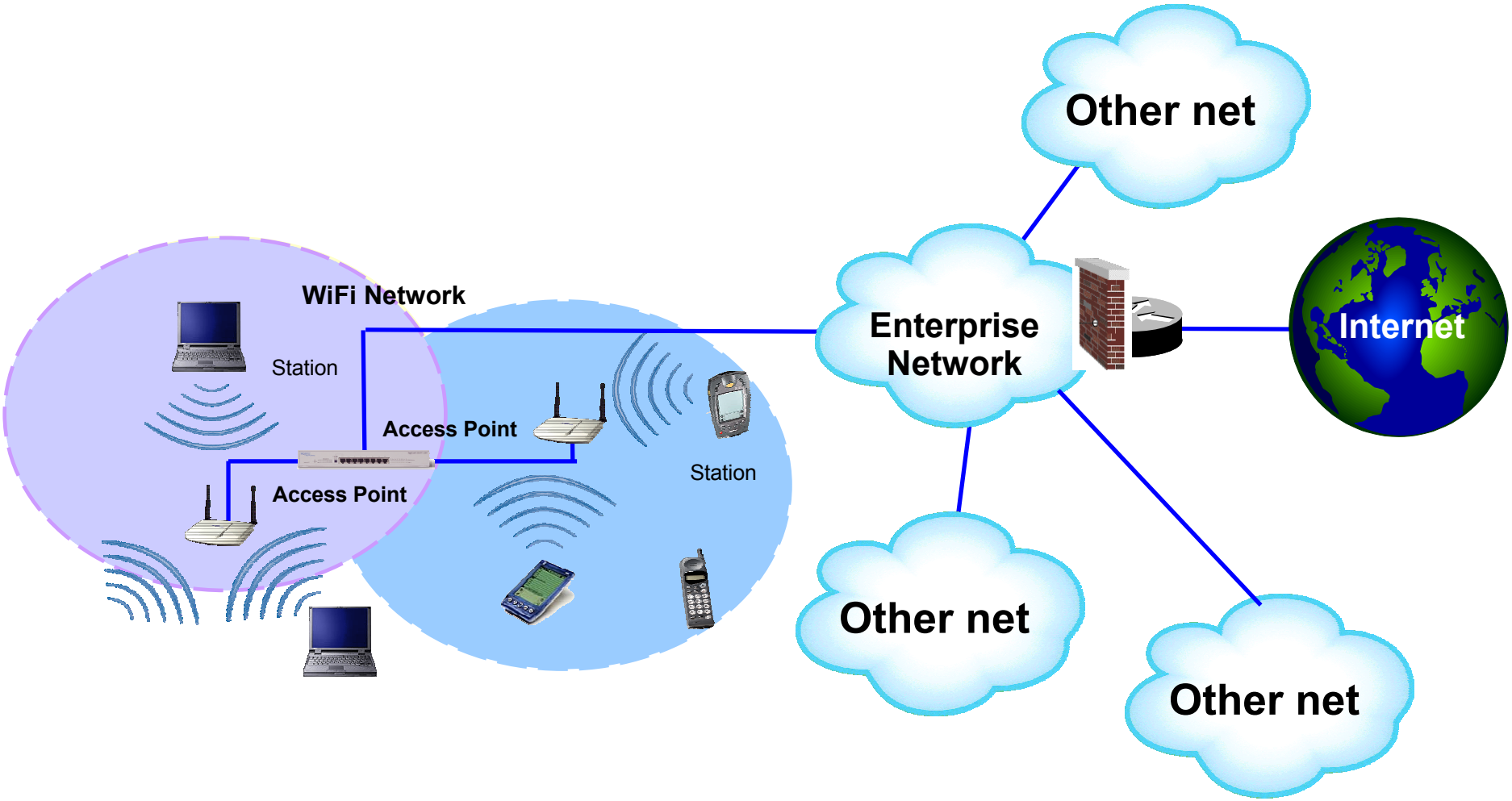


WiFi Privacy and Integrity

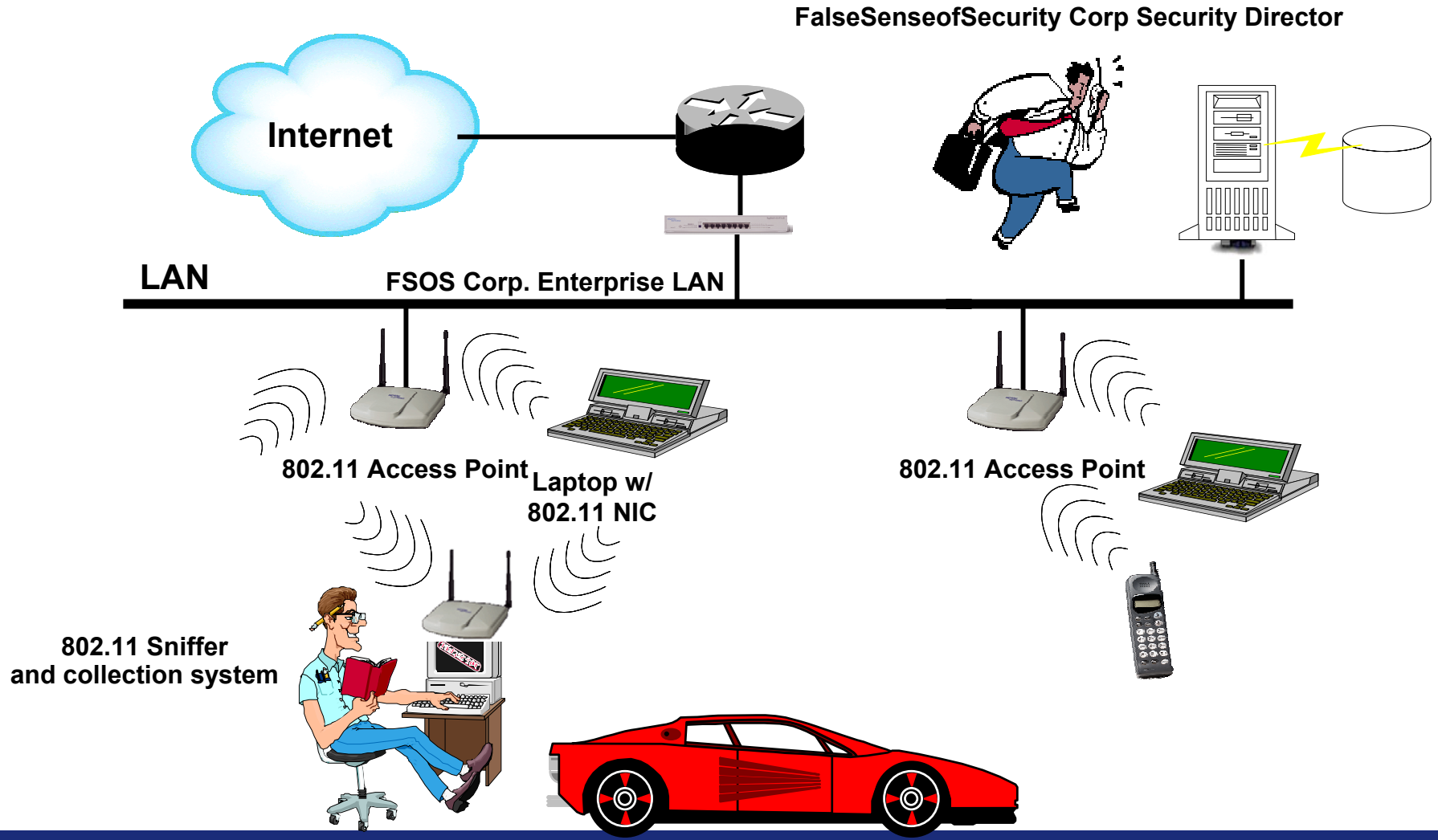


802.11 Security Vulnerabilities

Problem: Backdoor to the Enterprise



War-driving and War-chalking is plaguing technology



Possible Attacks & Vulnerabilities

- Eavesdropping – Eavesdropping on messages is possible
- Traffic Analysis – Who is communicating with whom
- Masquerade – Gaining access to an enterprise network and beyond
- Replay – Capture of legitimate messages is possible and may be played back
- Message Modification – Adversary may be able to modify messages captured
- Denial-of-Service – Jamming of wireless devices is possible or denying service

Key Security Problems with WiFi

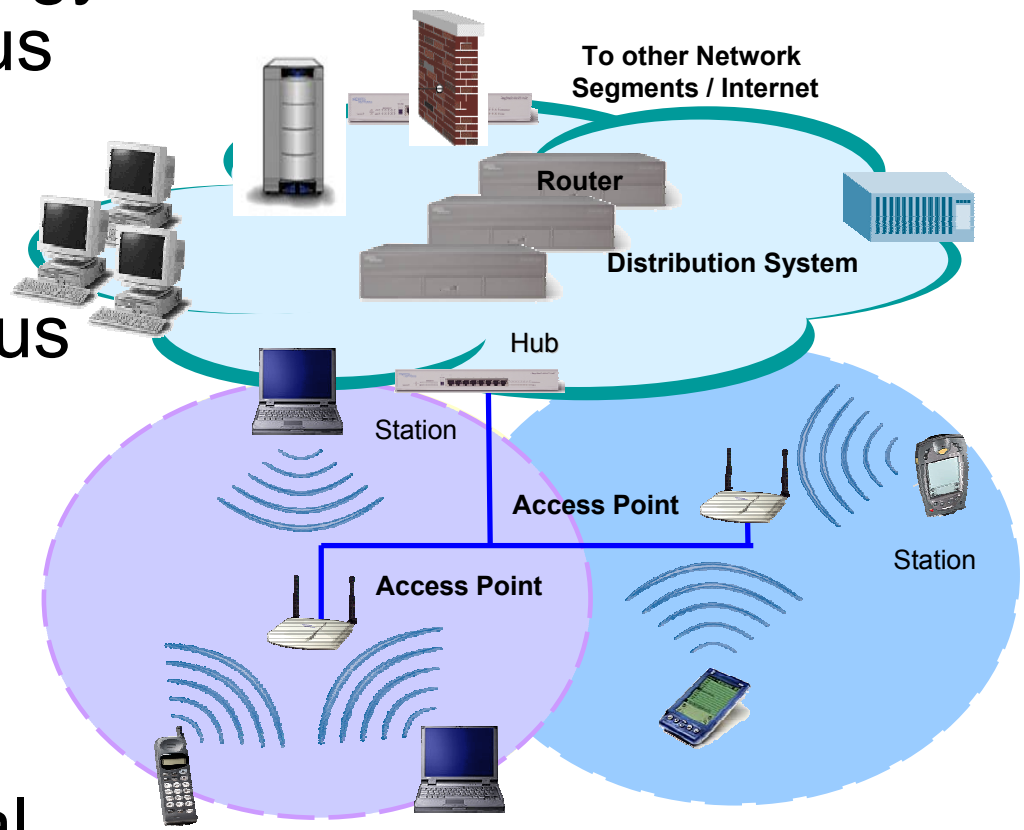
- Security features in vendor products are frequently not enabled.
- IVs are short (or static).
- Cryptographic keys are short.
- Cryptographic keys are shared.
- Cryptographic keys cannot be updated automatically and frequently.
- RC4 is used inappropriately used in WEP.

Key Security Problems with WiFi

- Packet integrity is poor.
- No user authentication occurs.
- Authentication is not enabled; only simple SSID identification occurs.
- Device authentication is simple shared-key challenge-response.
- The client does not authenticate the AP.

802.11 Brings Security Concerns

- This tetherless technology is attractive for numerous reasons.
- "Out of the box" technology has numerous flaws.
- Very risky without vigilance.
- Secure design and implementation is critical.



NIST Special Publication 800-48

The document examines the benefits and security risks of 802.11 Wireless Local Area Networks (WLAN), Bluetooth Ad Hoc Networks, and Handheld Devices such as Personal Digital Assistants (PDA). The document also provides practical guidelines and recommendations for mitigating the risks associated with these technologies.

http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

NIST FIPS140-2 Validation

" is mandatory and binding for federal agencies that have determined that certain information be protected via cryptographic means."

- Title is *Security Requirements for Cryptographic Modules*
- Specifies requirements for a cryptographic module used within a security system protecting sensitive information
- Four levels of security (Level 4 is highest)
- Covers 11 topical areas (ports and interfaces, physical security, self-tests, finite state model, operational environment, etc.)

Best Practices

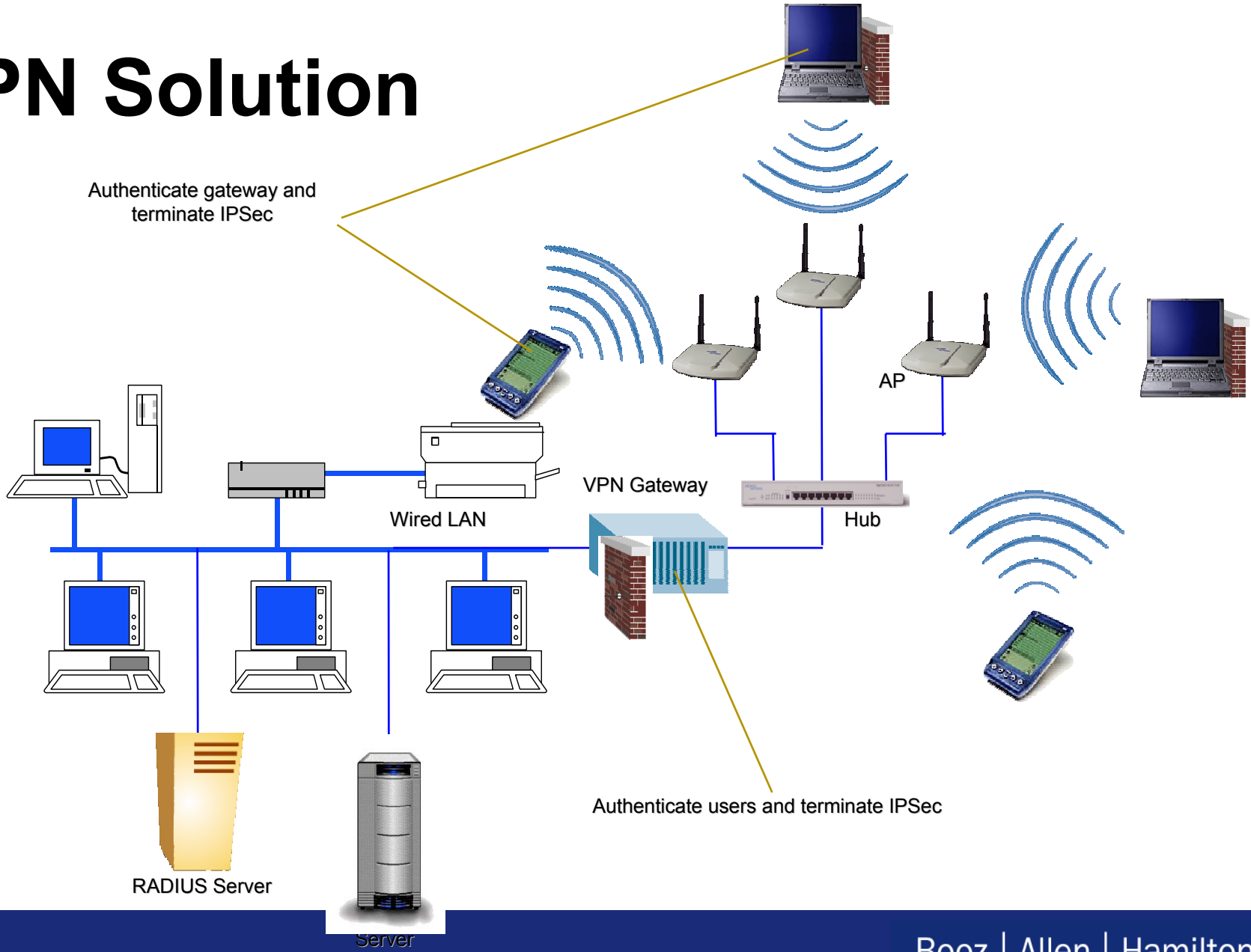
- Ensure you understand and can manage risks to the organization
- Be aware of the implications of wireless and handheld devices
- Carefully plan the deployment of Bluetooth, WiFi and all wireless technologies
- Be vigilant with implementing management practices and controls
- Ensure proper physical controls are in place
- Assess risks and test security frequently

Security Solutions for 802.11

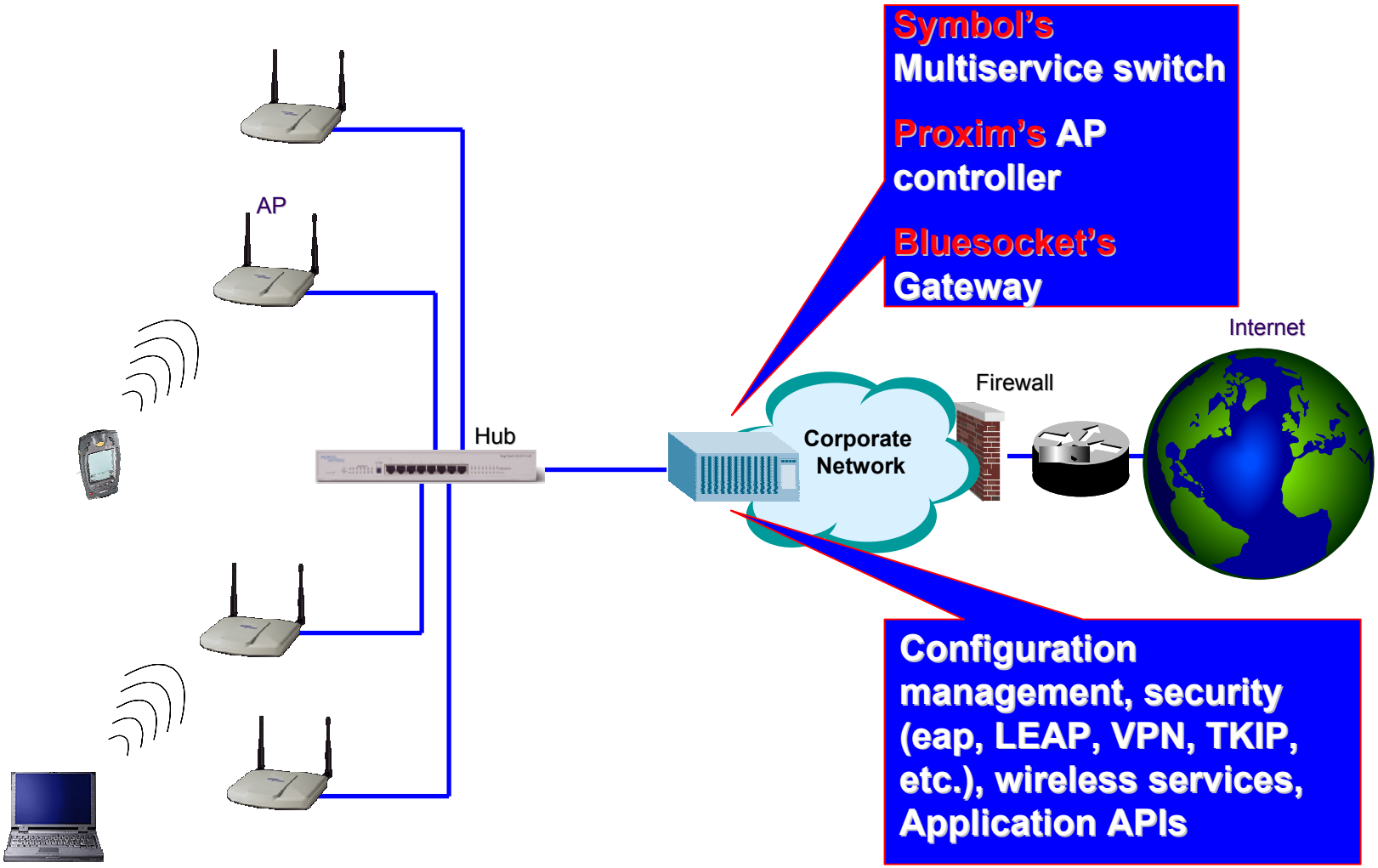
802.11 Security Solutions Abound

- Do nothing or use WEP security
- WEP security with patches
- Layer 2 (Type-1) replacement for RC4/WEP
- Layer 3 VPN based on IPsec
- LEAP (Lightweight Extensible Authentication Protocol)
- Security switch with “add-ons” to address other security services
- IETF Solutions based on EAP (eap-TTLS, eap-TLS, eap-GSM, etc.)
- WiFi Protected Access (WPA)
- Robust Security Network (RSN)

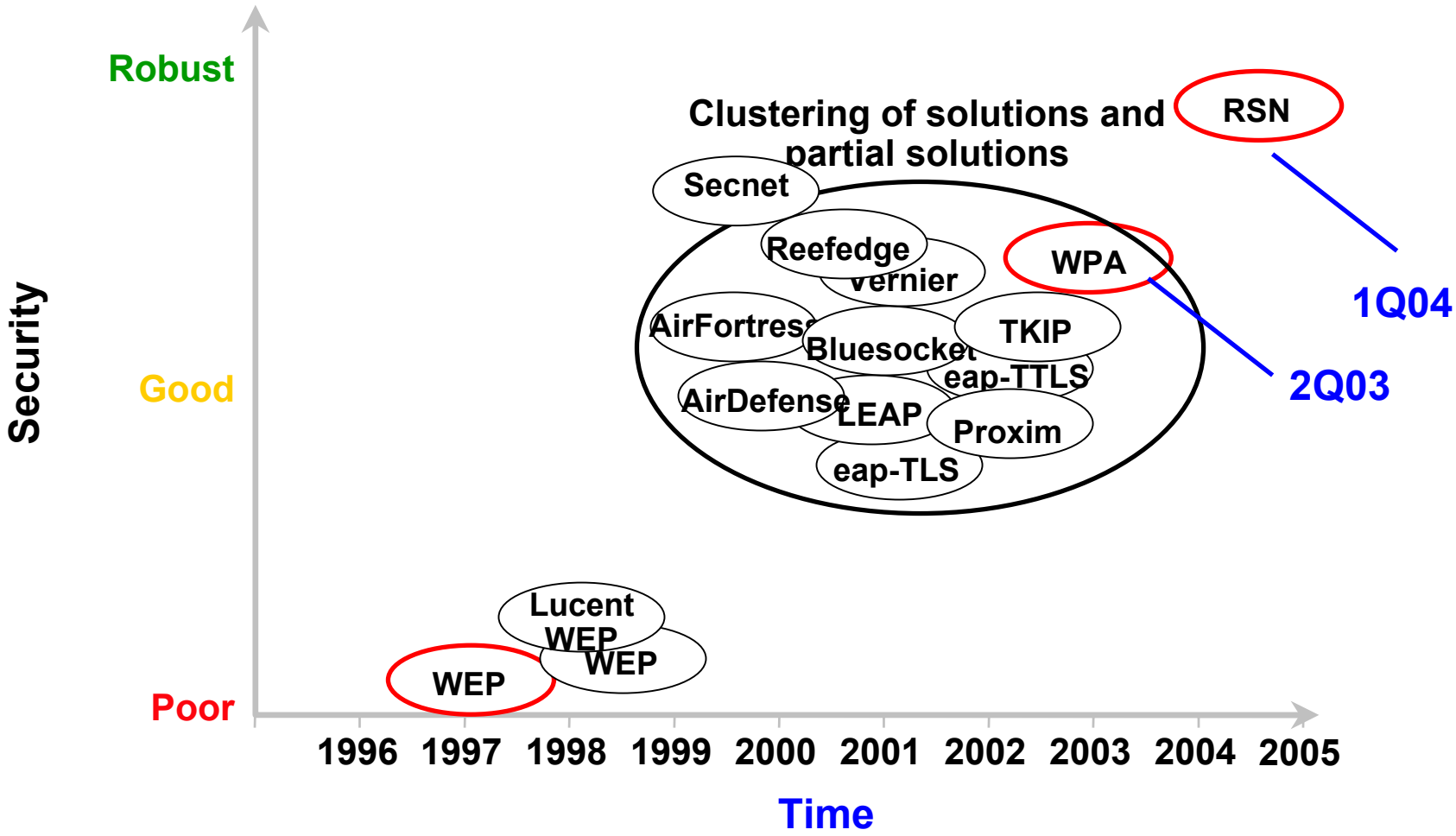
VPN Solution



New Model for 802.11 Security – Wireless Security Gateway



Evolution of WiFi Security Solutions/Stds (Illustrative only)



WiFi Protected Access (WPA)

- Project grew out of initiative that started earlier this year to address WEP problems
- Includes Microsoft, Symbol, Cisco, Agere, Proxim, Intersil
- Key features include:
  - TKIP (Temporal Key Integrity Protocol)
  - 802.1X port-based access control
  - PEAP (Protected EAP Protocol)
- Seeks to embrace TKIP and security features ahead of IEEE ratification

Robust Security Networks

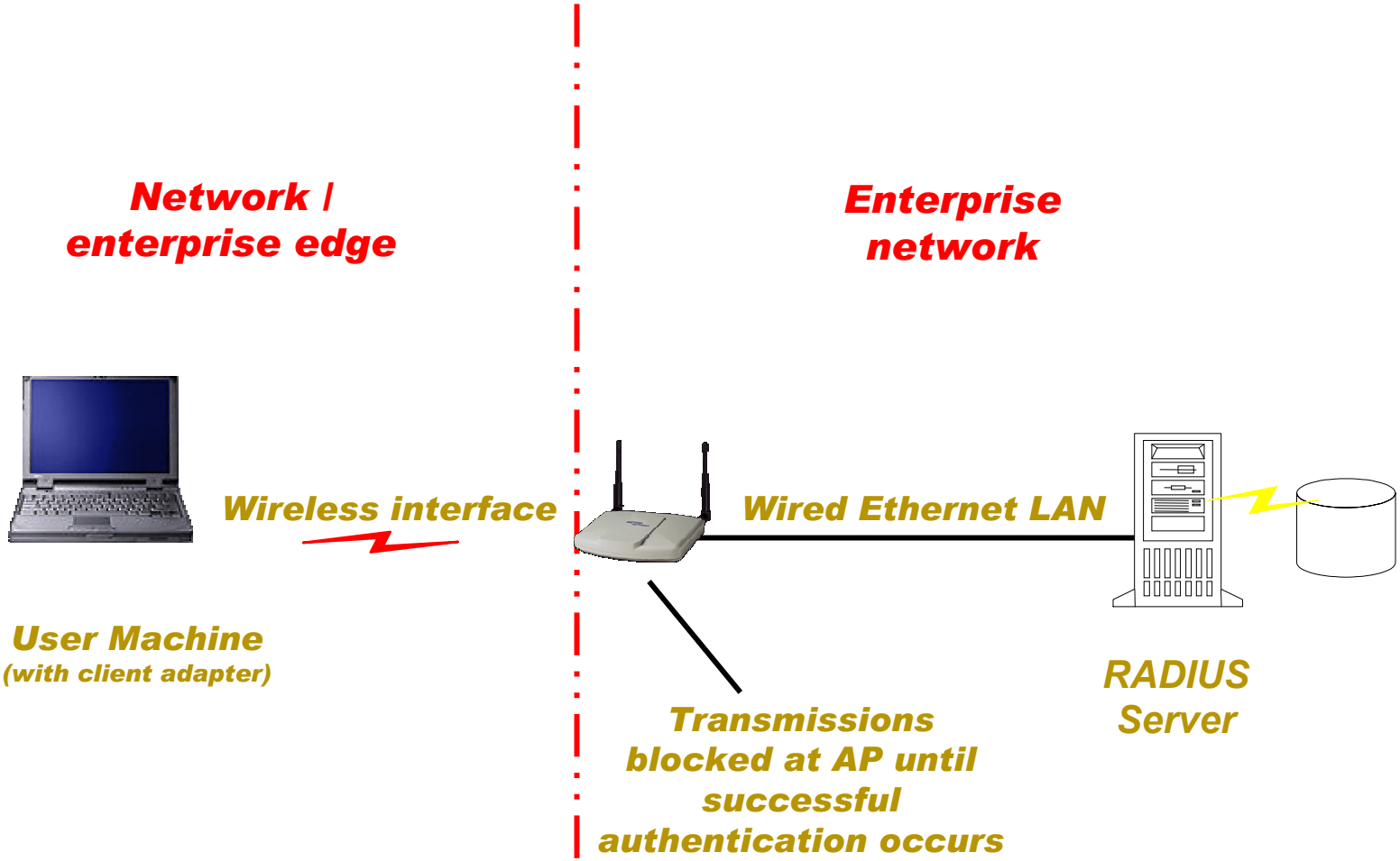
- Long-term security solution for 802.11 WLANs
- Developed by IEEE 802.11 Task Group i (TGi)
- Will apply to 802.11a, 802.11b and 802.11g
- Will fix the known, existing problems with WEP
- Key security features include:
  - Mutual authentication using Extensible Authentication Protocol (EAP) techniques
  - 802.1X port-based access control
  - Confidentiality using Advanced Encryption Standard
  - Replay protection
  - Data origination authentication and Key management

Some Relevant Security Standards

- FIPS PUB 140 – Security for Crypto Modules
- FIPS PUB 197 – Advanced Encryption Standard
- FIPS PUB 180 Secure Hash Standard
- IEEE 802.1X – Port-based access control
- RFC2104 – Keyed Hashing for Message Authentication (HMAC)
- RFC3394 – AES Key Wrap Algorithm

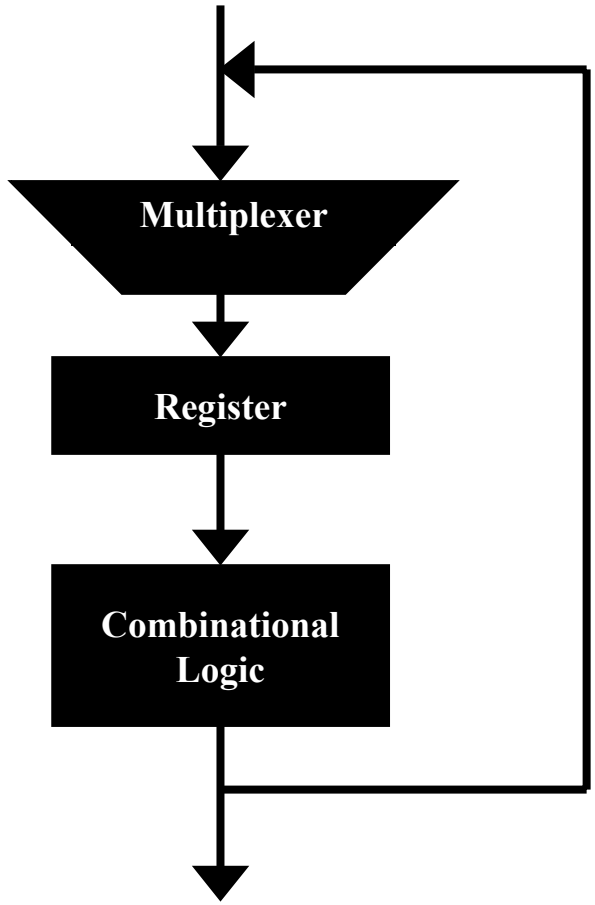
RSN requires numerous standards

Topology of 802.1X port-based access control



Advanced Encryption Standard (AES)

- Is an iterated block cipher
- Will be used for confidentiality and integrity
- Is NIST's latest approved cryptographic algorithm
- Defined by Federal Information Processing Standard (FIPS) 197

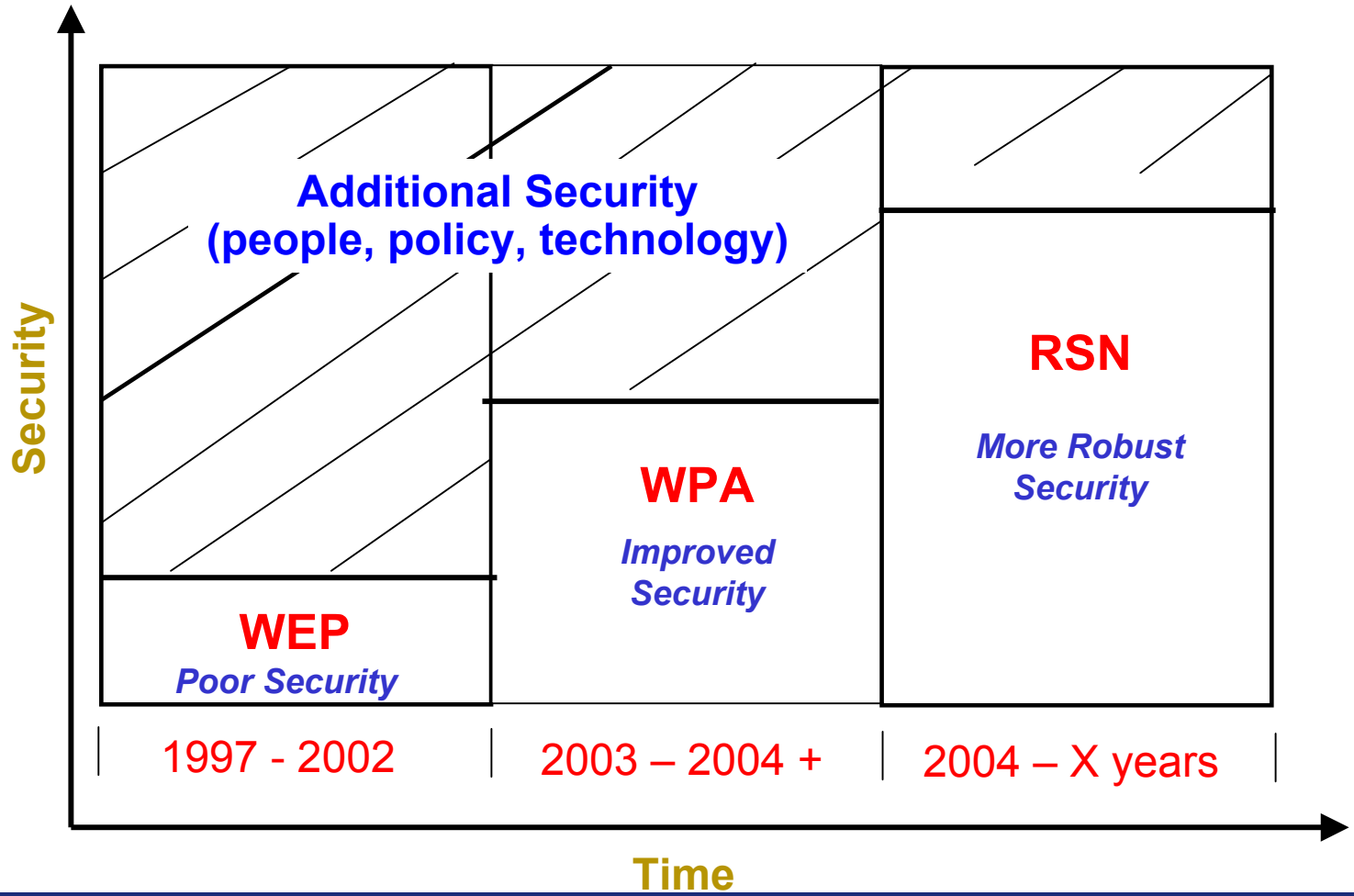


Evolution of WiFi Security (IEEE)

Security Feature	Wired Equivalent Privacy (WEP)	WiFi Protected Access (WPA)	Robust Security Networks (RSN)
Encryption Algorithm	RC4	RC4	**AES**
Key Management	None	EAP-based	**EAP-based**
Cryptographic Keysize	40-bit or 104-bit	128-bit (64-bit for authentication)	**128-bit**
Packet Key	Created by Concatenation	Created by mixing function	**Not needed**
Data/Header Integrity	CRC-32 / None	Michael Algorithm	**CCM**
Cryptographic Key life	24-bit, wrap	48-bit	**48-bit**
Replay protection	None	Uses IV	**Uses IV**

Key: AES = Advanced Encryption Standard; CCM = Counter Mode with CBC-MAC (AES-based); EAP = Extensible Authentication Protocol; IV = Initialization Vector; RC4 = Rivest Cipher 4.

WiFi Security



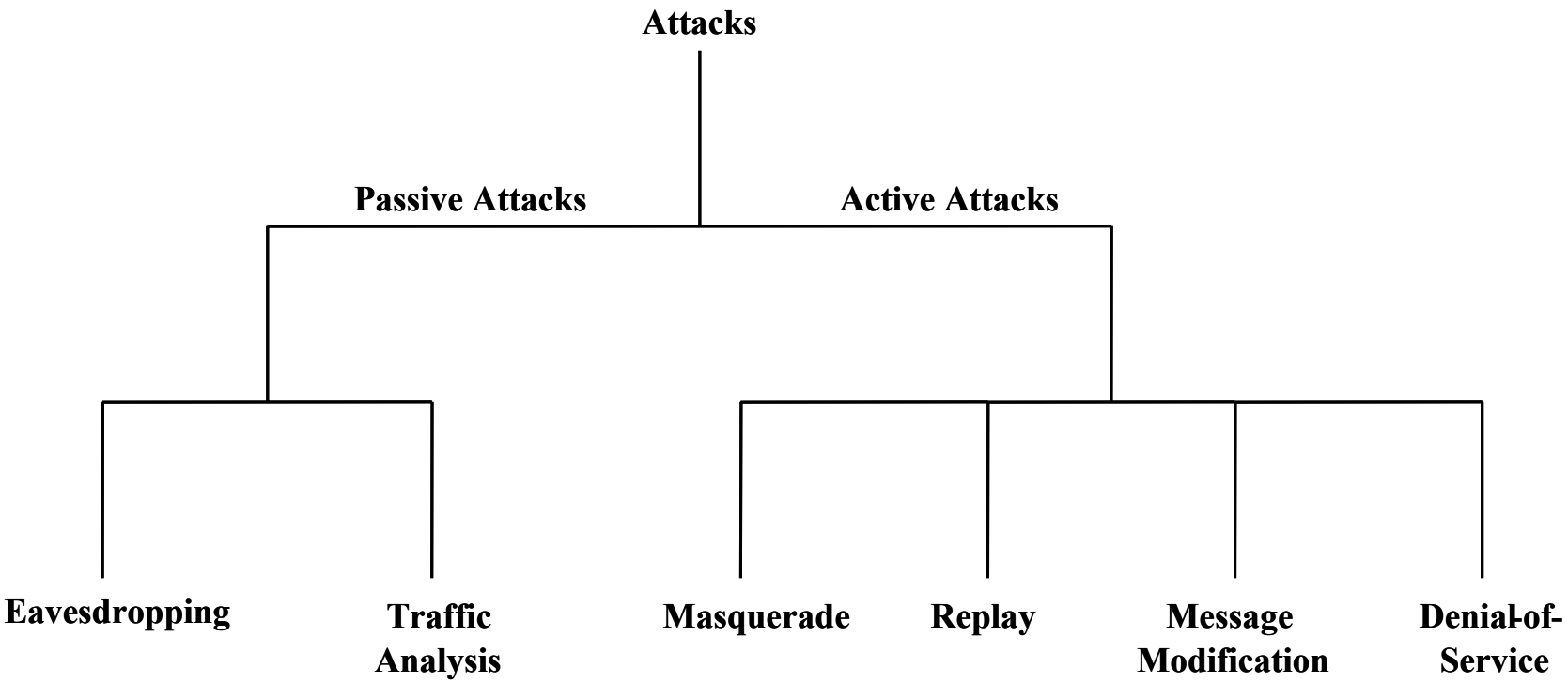
Important WiFi Security Event and Site

On 4th and 5th December 2002, the National Institute of Standards and Technology (NIST) held a workshop on 802.11 Wireless LAN Security. The workshop comprised approximately 30 individuals from the US Federal Government, the WiFi industry and the security academic communities. For details on WiFi security and the event, visit:

http://csrc.nist.gov/wireless/

Comprehensive Wireless Security Solutions

General Attack Taxonomy for Wireless



Wireless is particularly vulnerable to these

What are the required services for the wireless environment?

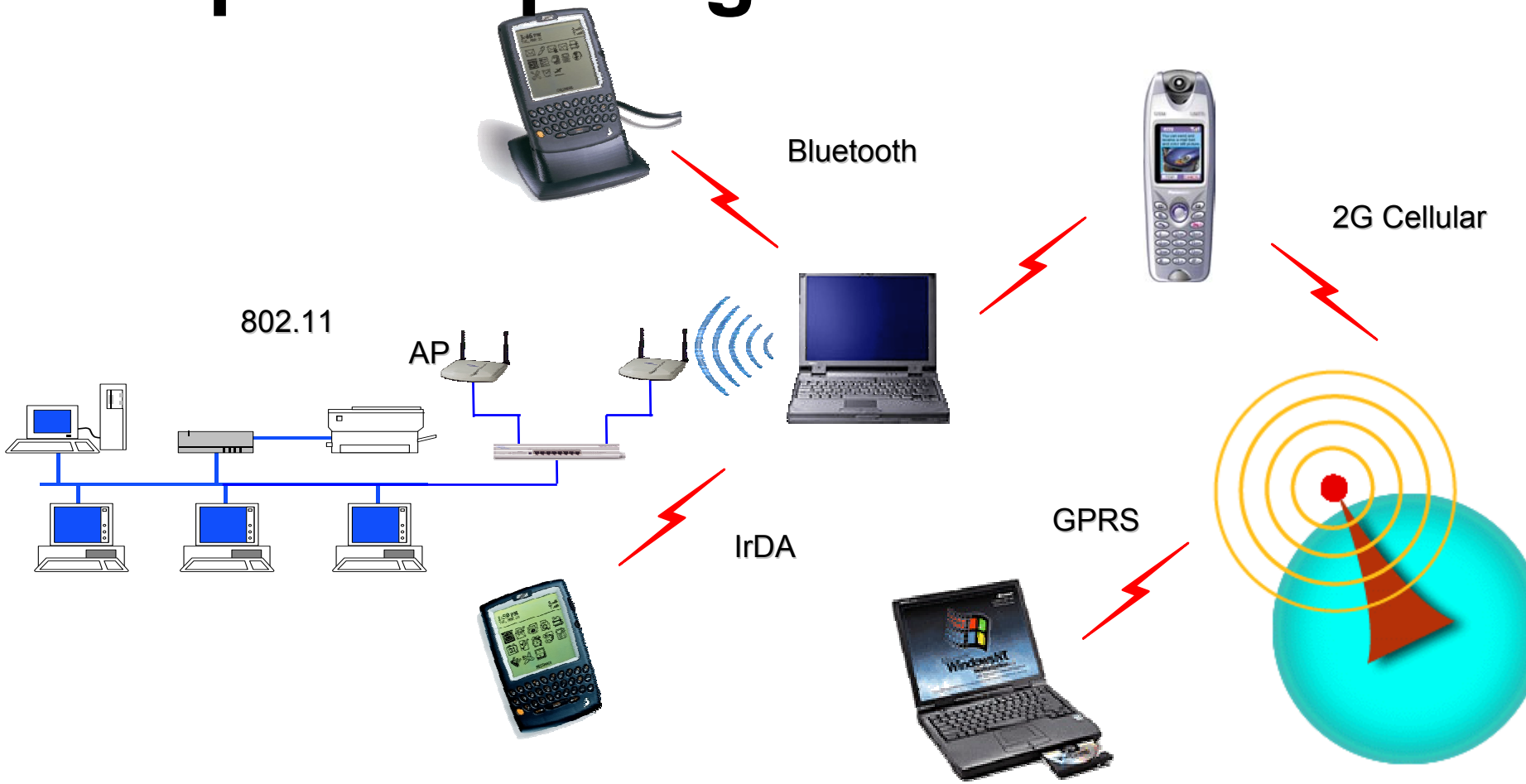
- Access Control
- Audit
- Authentication
- Availability
- Confidentiality (privacy)
- Integrity
- Key Management
- Non-repudiation

Security – Big Three

- *Confidentiality* – ensures that only authorized individuals and parties can access information in a computer system or communications network.
- *Integrity* – ensures that only authorized individuals and parties can modify information in a computer system or communications network. Integrity includes changing, deleting, inserting, or delaying information.
- *Availability* – ensures information is available for use when, where and in the form required.

Future Wireless

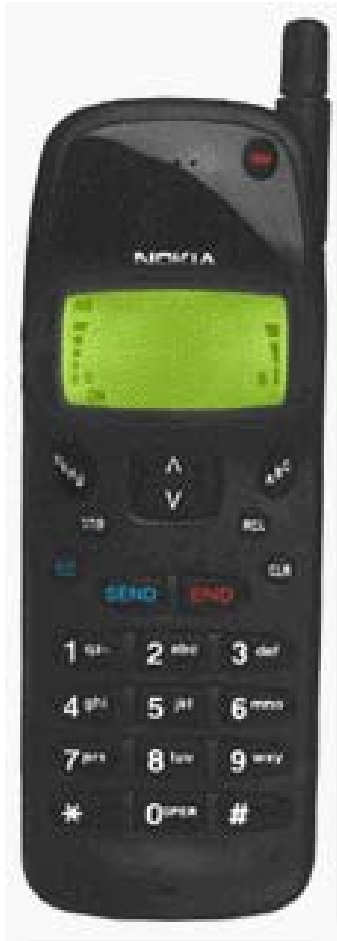
Complex Topologies



Complex wireless topologies are possible that increase the security risks

5 Key Technologies on the Horizon

- Software Defined Radio (SDR)
- UltraWide Band (UWB)
- Mesh and Ad Hoc Networks
- Wireless Personal Area Networks
- Adaptive radio



History Repeats Itself

	WiFi	1st Generation Cellular
Time Period	2002	1992
State of industry	Exploding	Exploding
State of security	Poor	Poor
Buzzwords	War-driving and war-chalking	Counterfeiting / cloning
Tools of choice	Netstumbler and Airsnort	Curtis ESN reader and Timson software
Detectability	Difficult.	Difficult a priori. Easy after the customer complains
Triage solution	Patched WEP, VPNs	PINs, clone detectors, RF fingerprinting
"Hot" solution to the problem	Switch-based security devices	RF fingerprinting

Some Lessons-learned for Wireless

- We must learn from our past mistakes
- Robust, well-implemented cryptography is a must
- Key distribution and management need to be considered carefully and cannot be ignored
- Users must be vigilant with wireless – know the risks *before* deployment
- With security – the devil is in the details
- A comprehensive program must exist to address all aspects of security (physical, logical, person.)

Discussion

Presenter Information

Leslie D. Owens (Les)

Booz Allen Hamilton, Wireless Security Lead

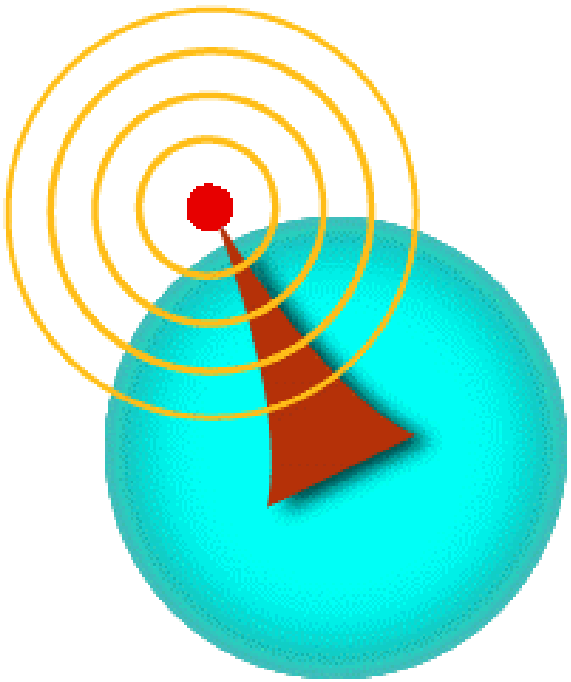
703/902-7091 (office)

703/980-3877 (cellular)

Owens_les@ bah.com (email)

les.owens@att.net

"Five or ten years from now, we won't worry about communication with wires, you'll just open you'll laptop or PDA and the data will be there"



Teresa Meng
Professor, Stanford and founder, Atheros

Backup Material

Types of Wireless Networks

- WWAN – Wireless Wide-Area Networks
- WLAN – Wireless Local Area Network
- WPAN – Wireless Personal Area Network

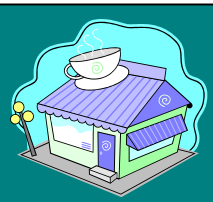
Wireless Adversaries (Threats)

Some of the adversaries (or threats)

- Hackers
- Thieves (fraudsters)
- Competitors
- Vandals
- Terrorists
- Foreign governments

Opportunities for Hotspots

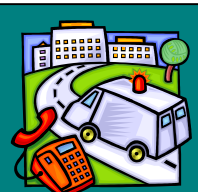
- Sports arenas



- Coffee shops & restaurant

- Theme parks

- Universities / Schools



- Hospital / Medical centers

- Hotels

- Museums/ Libraries

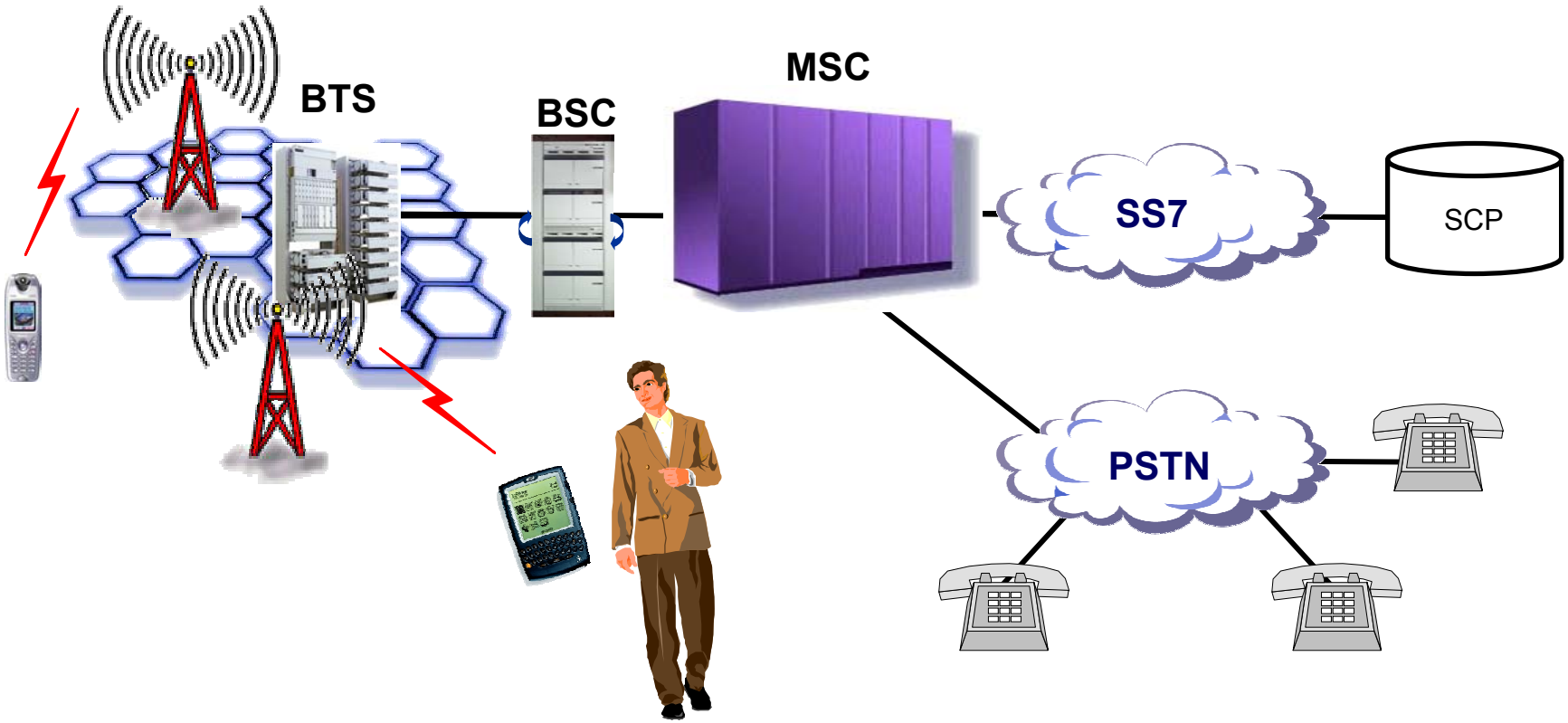
- Airports/Rail stations

- Shopping malls

Most people spend significant time in hotspots

This presents a tremendous business opportunity

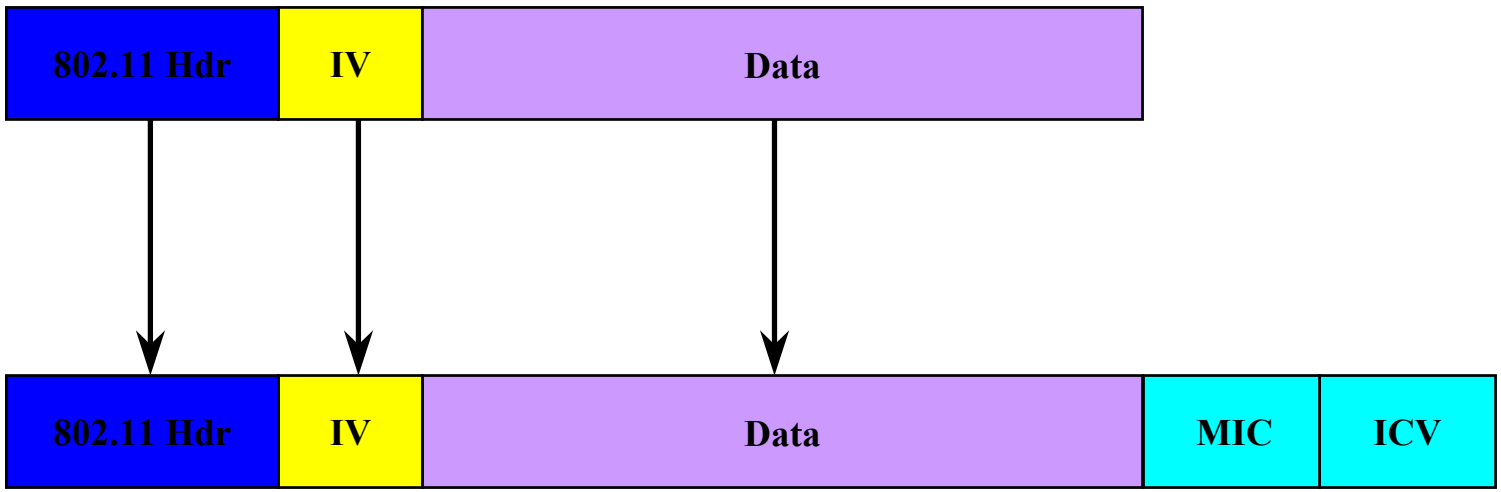
Third Generation Cellular



Temporal Key Integrity Protocol

- Fixes all known WEP vulnerabilities
- Mandates four new algorithms
  - Message Integrity Check (MIC) called Michael
  - New per-packet key construction with large IV
  - IV sequencing
  - Key distribution
- Accommodates existing hardware so upgrades can be made
- Solution minimizes performance degradation but with less-than-bullet-proof security

Michael Message Integrity Check to Defeat Forgeries



MIC: Michael (Key, Src-Addr || Dest-Addr || Data)

ICV: CRC (Data || MIC)

Security Definitions

- *Access Control* – This security service ensures that controls exist for accessing computer system information. The controls may be provided by or for the system.
- *Audit* – ensures that transactions are recorded in a journal (audit trail). An audit trail is typically a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of events (environments and activities) leading to an operation, procedure, or event in a security-related transaction from beginning to end.

Security Definitions

- *Authentication* – ensures that the origin of a message or electronic document is correctly identified and provides assurance that the identity is correct. Authentication also means that an entity (e.g., a user, process, or computer system) is properly identified.
- *Authorization* – is the right or permission that is granted to a user, program, or process to access a system resource

Security Definitions

- *Confidentiality* – ensures that only authorized individuals and parties can access information in a computer system or communications network. This access includes copying, displaying, printing, and other forms of disclosure.
- *Integrity* – ensures that only authorized individuals and parties can modify information in a computer system or communications network. Integrity includes changing, deleting, inserting, or delaying information in transmitted messages or stored messages.

Security Definitions

- *Key management* – is the process of handling cryptographic keys and related material (e.g., initialization values, counters) during their life cycle in a cryptographic system, including ordering, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the material. **N.B.**: this process (security service) is probably the most critical service a cryptographic system. It is oftentimes the most difficult part of cryptosystem design and operation; moreover, it is frequently poorly done or not done at all.